STATE OF INDIANA

DIVISION OF
STATE COURT ADMINISTRATION

SUPREME COURT

30 SOUTH MERIDIAN STREET SUITE 500
INDIANAPOLIS, IN 46204-3568
(317) 232-2542
FAX (317) 233-6586
www.IN.gov/judiciary

RANDALL T. SHEPARD, CHIEF JUSTICE

LILIA G. JUDSON, EXECUTIVE DIRECTOR
DAVID J. REMONDINI, CHIEF DEPUTY EXECUTIVE DIRECTOR

February 23, 2009

Mr. Michael J. Staresnick
Estate Recovery Manager
Office of Medicaid Policy and Planning, MS07
Indiana Family & Social Services Administration
402 W. Washington Street, Room W382
Indianapolis, IN 46204-2739

Dear Mr. Staresnick:

Your request to obtain bulk distribution of data from Indiana trial courts has been approved by the Division of State Court Administration pursuant to Administrative Rule 9(F), subject to the terms of the User Agreement for Bulk Distribution of Data. At this time, the Division has only approved the release of bulk records that are otherwise available to the public.

An executed copy of your user agreement is enclosed. This agreement will expire on January 31, 2010. Also enclosed is a distribution receipt form that must be completed and returned to this office within thirty (30) days of receiving bulk distribution of court records. If you have any questions, please contact staff attorney Kristin Donnelly-Miller of our office or me.

Sincerely,

James R. Walker

James R. Walker
Director of Trial Court Management

Enclosure

Indiana Supreme Court
Division of State Court Administration

USER AGREEMENT FOR BULK DISTRIBUTION OF DATA OR COMPILED INFORMATION NOT EXCLUDED FROM PUBLIC ACCESS UNDER ADMINISTRATIVE RULE 9

The Indiana Supreme Court through its Division of State Court Administration ("Division") and Indiana Family and Social Services Administration ("Requesting Party") hereby enter into this User Agreement for Bulk Distribution of Data or Compiled Information ("Agreement") for the purpose of establishing roles and responsibilities associated with the dissemination and use of Indiana court information pursuant to the provisions of Administrative Rule 9 of the Indiana Rules of Court ("Rule 9").

Recitals

A. Pursuant to Rule 9(F)(2), the Division is responsible for approving all requests for bulk distribution of Data or Compiled Information by Indiana Courts.

B. The Division reviews each request for bulk distribution to insure that the request is consistent with the purposes of Rule 9 and that each request is an appropriate use of public resources.

C. The Requesting Party seeks bulk distribution of Data or Compiled Information for its own use and understands that it must comply with the provisions of this Agreement.

D. The Division requires that the Requesting Party understand and agree to comply with certain restrictions on usage of the Data and Compiled Information.

E. The Requesting Party is not automatically entitled to the distribution of Data or Compiled Information of a county simply by the approval of this user agreement by the Division.

F. The Requesting Party will be required to pay reasonable costs incurred by the Division or by the responding Court/Clerk in responding to the request for bulk distribution.

G. The bulk distribution is limited to court records, even if the Requesting Party is seeking other information that is governed by other agencies' policies.

Agreement

1. **Definitions**. For the purpose of this Agreement, the following definitions shall apply:

   A. "Administrative Record" means any document, information, data, or other item created, collected, received, or maintained by a Court, Court agency, or Clerk of

Court pertaining to the administration of the judicial branch of government and not associated with any particular case or other agency.

B. "Agreement" means this User Agreement for Bulk Distribution of Data or Compiled Information, as well as any attachments or exhibits that may be affixed to this document or referenced within the agreement.

C. "Bulk Distribution" means the distribution of all, or a significant subset of Court Records not excluded from public access, in electronic form if possible, as is, and without modification or compilation.

D. "Case Record" means any document, information, data, or other item created, collected, received, or maintained by a Court, Court Agency or Clerk of Court in connection with a particular case, not otherwise governed by Rule 9(G) or (H).

E. "Clerk of Court" means the Clerk of the Indiana Supreme Court, Court of Appeals and Tax Court, the Clerk of a Circuit, Superior, Probate or County Court, the Clerk of a City or Town Court, and the Clerk of a Marion County Small Claims Court, including staff.

F. "Compiled Information" means information that is derived from the selection, aggregation or reformulation of all or a subset of all of the information from more than one individual Court Record in electronic form in response to the approved request for bulk distribution.

G. "Court" means the Indiana Supreme Court, Court of Appeals, Tax Court, and all Circuit, Superior, Probate, County, City, Town, or Small Claims Courts as well as any division, section, office, unit, or other entity of the Court, as well as any of the officers, officials, employees, volunteers, contractors, or others acting as representatives lawfully representing the Court.

H. "Court Records" means both Case Records and Administrative Records.

I. "Data" means any computer or machine-readable copy of Court Records provided by a Court to the Requesting Party.

J. "Subscriber" means a client or customer of Requesting Party to whom bulk Data or compiled information is provided or to whom access to bulk Data or Compiled Information is given.

K. "Public Access" means the process whereby a person may inspect and copy the information in a Court Record, not excluded by Rule 9(G) or (H).

L. "Requesting Party" includes the above-identified party and all entities and known names under which the business operates, all subsidiaries that will utilize the Data or Compiled Information provided and all names under which subsequent individual requests to counties shall be made.

2. **Grant**. Subject to permission from the counties or Courts identified below, the Division hereby grants to the Requesting Party restricted authorization to receive from such counties or Courts the Court Records specifically identified below for the Requesting Party's use in accordance with the terms and conditions contained herein.

Execution of this Agreement and approval of the Requesting Party's request by the Division do not create any mandatory obligation on the part of any county or Court to provide Court Records to the requesting Party. Pursuant to Administrative Rule 9(F), the counties or Courts identified below must determine on an individual basis whether resources are available to transfer the Court Records to the Requesting Party and whether fulfilling the request is an appropriate use of public resources. Counties and Courts must determine on an individual basis whether to assess a reasonable charge and the amount of that charge for providing the Court Records to the Requesting Party.

A. **Court Records sought**:

Probate estates both supervised and unsupervised, Trust, and Guardianships

B. **Requested Counties**: ALLEN, FRANKLIN, SHELBY

Bartholomew, Brown, Clay, Clinton, Davisess, Decatur, Deleware, DuBois, Elkhart, Fayette, Fountain, Fulton, Gibson, Grant, Hamilton, Hancock, Henry, Howard, Jay, Johnson, Kosciusko, LaGrange, LaPorte, Madison, Marshall, Miami, Montgomery, Morgan, Perry, Pike, Putnam, Randolph, Ripley, Spencer, Starke, Sullivan, Vigo, Wabash, Warrick, Wayne, Wells, White, Whitley.

3. **Rights and Interests**. All rights, title and interests in and to the Court Records including all intellectual property rights therein shall remain with the counties or Courts. The Requesting Party shall not gain any proprietary right to or interest in any Court Records provided to the Requesting Party as a result of this Agreement. All rights, title and interests in materials created by or for Requesting Party for use in connection with the Court Records including all intellectual property rights therein shall be owned by the Division and the Requesting Party hereby assigns such rights, title and interests to the Division. Those rights may not be transferred, assigned, or sold for any purpose to any person, corporation, partnership, association, or organization of any kind. The Requesting Party shall provide the Division with the names of all entities related in any way to the Requesting Party, including subsidiaries and affiliates, the names under which the Requesting Party is doing business and any other related entity names. The Requesting Party shall supplement this agreement within thirty (30) days of a change in the list of names provided to the Division as requested by this Section 3.

4. **Ongoing Data Scrubbing and Update Requirements**. The Requesting Party shall comply fully with Rule 9 and shall delete any Social Security Number, bank account number and any other confidential information that is inadvertently included in the Court Records and take other appropriate action to ensure that such confidential information is not disclosed to others. Upon notice, the Requesting Party shall comply with future orders to scrub data if they should arise.

5. **Restrictions on Use of Data.**

A. **Compliance With Authorities**. The Requesting Party shall comply with all current and, as subsequently amended, federal and state laws, court rules, administrative rules and policies governing, regulating, and/or relating to Court Records.

B. **Resale of Data**. Except as set forth in Section 6, the Requesting Party shall not reproduce, resell or otherwise distribute the Court Records or Data provided pursuant to this Agreement except in response to an inquiry from an individual for a Court Record or compilations or reports incidental to such individual Case Record as part of a service provided by Requesting Party. The Requesting Party shall not reconfigure the Court Records for subsequent bulk distributions.

C. **Policies for dissemination of Data**. The Requesting Party shall not disseminate Court Records to the public through remote electronic access such as the Internet or other electronic method unless the County Clerk first obtains approval from the Division under Trial Rule 77(K). In the event the Requesting Party plans to offer a service allowing others to review the Court Records and disseminate information in the Court Records to subscribers, customers, clients, or other third parties, a current copy of the Requesting Party's policies and information related to the dissemination shall be attached hereto as an Exhibit B. The Requesting Party is under an ongoing obligation to provide the Division with a copy of any updated Policy information within thirty (30) days of its modification.

6. **Bulk Transfer to Third Parties**. If the Requesting Party has submitted a request to transfer bulk Data or Compiled Information to third parties as part of the Request attached hereto as Exhibit C and such request has been approved by the Division as part of the Approval Letter attached hereto as Exhibit D, then the Requesting Party may transfer the bulk Data and Compiled Information it is authorized to receive under this Agreement to such third party subject to the terms of this Agreement. The Requesting Party shall supplement its Request in Exhibit C with a copy of any Agreement entered into with the third party subject to the execution of this Agreement. The Requesting Party may not transfer bulk Data or Compiled Information to any third party who has not signed a User Agreement with the Division. The Requesting Party may not charge the third party any more than the amount for time and material set forth in Exhibit C.

7. **Reporting Requirement.** Within thirty (30) days after the Requesting Party has received the first or only distribution of Court Records, the Requesting Party shall file with the Division of State Court Administration the Distribution Receipt Form, attached hereto as Exhibit E (Form TCM-AR9(F)-3).

8. **Disclosure Requirements.** The Requesting Party shall provide a disclosure statement similar to the one set forth below to each subscriber, customer, client or other third party who is provided access to the Court Records at the time any information from the Court Records is made available to them. At a minimum, the Requesting Party will ensure that a statement similar to the one set forth below, is displayed or provided to each subscriber, customer, client or other third party every time information from the Court Records is made available.

The data or information provided is based on information obtained from Indiana Courts on N/A *(insert date most current version was created or in the case of data from multiple sources, the range of dates relevant to the displayed data). The Division of State Court Administration and the Indiana Courts and Clerks of Court: 1) Do not warrant that the information is*

accurate or complete; 2) Make no representations regarding the identity of any persons whose names appear in the information; and 3) Disclaim any liability for any damages resulting from the release or use of the information. The user should verify the information by personally consulting the official record maintained by the court in question.

Non-applicable. The agency will be a recipient of data and used to aid in the recovery of funds on behalf of the State of Indiana. The data received by the agency will not be distributed to any parties outside of the agency staff employed in recovery of funds.

9. **Audits.** The Division may, at its discretion, perform audits to verify compliance with the terms and conditions of this Agreement and the appropriate use of the Court Records. The Requesting Party shall cooperate with the Division in such audit.

   A. The Requesting Party agrees that the Division may include "control" or "salted" data as a portion of the Court Records as a means to ensure that any personally identifiable information is not used for commercial solicitation purposes or in an indiscriminate and reckless manner.

   B. The Requesting Party agrees to provide the Division with access, at no charge, to any database created using the Court Records for the purpose of monitoring and auditing contract compliance.

   C. The Requesting Party agrees to provide the Division with copies of the materials and information the Requesting Party provides its subscribers, customers, clients, or other third parties.

10. **Disclaimer of Warranties.** The Division, Courts, and Clerks of Court provide no warranties, express or implied and specifically disclaim without limitation any implied warranties of merchantability and fitness for a particular purpose, with respect to the Court Records or Data provided under this Agreement. All Court Records and Data provided under this Agreement is provided "As Is". The Division, Courts, and Clerks of Court further provide no warranties, express or implied, that the Court Records or Data is accurate, current, correct, or complete. It is expressly understood that it is the responsibility of the Requesting Party and/or its subscribers, customers, clients, or other third parties to whom the Court Records and Data is supplied to verify the Court Records and Data with the official information maintained by the Court having jurisdiction over the Court Records. **Reproductions of the Court Records or Data provided to the Requesting Party shall not be represented as a certified copy of the Court Record.**

11. **Limitation of Liability.** The Requesting Party acknowledges and accepts that the Court Records or Data may include errors or omissions and, therefore the Requesting Party agrees, that the Division, Courts, and Clerks of Court shall not be responsible or liable in any way whatsoever for the validity of the Court Records or Data. Specifically:

A. The Division, Courts, and Clerks of Court shall not be liable for any demand or claim, regardless of the form of action, for any damages resulting from the use by the Requesting Party or any of its subscribers, authors, clients or other third parties of the Court Records or Data.

B. The Division, Courts, and Clerks of Court shall not be liable for any demand or claim, regardless of form of action, for any damages arising from incorrect or incomplete information provided under this Agreement.

C. The Division, Courts, and Clerks of Court shall not be liable to the Requesting Party or any other party for any loss, including revenue, profits, time, goodwill, computer time, destruction of data, damages or any other indirect, special or consequential damage which may rise from the use, operation, distribution, transfer or modification of the Court Records or Data.

12. **Indemnification.** The Requesting Party shall defend, indemnify, and hold harmless the Division, Courts, and Clerks of Court, their respective employees and agents, and the State of Indiana from and against all claims, demands, suits, actions, judgments, damages, loss or risk of loss (including expenses, costs, and attorney fees) of any and every kind and by whomever and whenever alleged or asserted arising out of or related to any use, distribution or transfer made of the Court Records or Data by the Requesting Party or any of its subscribers, customers, clients or third parties.

13. **Assignment.** The Requesting Party may not, without the express written permission of the Division, transfer or assign: (i) this Agreement or any portion thereof; (ii) any right or benefit accruing to the Requesting Party under this Agreement; nor (iii) any claim arising under this Agreement.

14. **Termination and Renewal.**

A. **General.** Either the Division or the Requesting Party upon thirty (30) days written notice may terminate this Agreement without cause.

B. **Renewal.** This agreement expires on January 31, ~~2009~~ 2010, subject to renewal upon request by the Requesting Party. Renewal Requests may be sent to the Division after January 1, ~~2009~~ 2010. The renewal shall be for one calendar year. The Division will post the Renewal Form on the Supreme Court website at www.in.gov/judiciary/admin/forms/admin/index.html.

C. **Termination for Cause**. The Requesting Party shall be responsible and liable for any violations of this Agreement by the Requesting Party or any officer, employee, agent, subscriber, customer, or client of the Requesting Party or any third party to whom the Requesting Party has transferred bulk Data or Compiled Information and any such violation shall result in immediate termination of this agreement by the Division, at which time all Court Records and Data supplied to Requesting Party or any officer, employee or agent of the Requesting Party in any form will immediately be returned to the Division. In such event, the Requesting Party shall be liable for damages as authorized by law.

D. **Termination for Nonpayment.** The Division may immediately, without notice, terminate this Agreement for failure of Requesting Party to pay an invoice for costs associated with the preparation or transfer of the Court Records and Data outstanding longer than 30 days.

E. **Termination in Event of Assignment.** The Division in its sole discretion may terminate this Agreement without notice if the Requesting Party transfers or assigns, without the express written permission of the Division: (i) this Agreement or any portion thereof; (ii) any right or benefit accruing to the Requesting Party under this Agreement; nor (iii) any claim arising under this agreement.

F. **Termination in Event of Failure to Update.** The Requesting Party is under an ongoing obligation to provide the Division with a complete list of entities and names under which the Requesting Party conducts business. The Division, in its sole discretion, may terminate this Agreement if the Requesting Party does not update any of the information required to be submitted in the Request attached as Exhibit C.

15. **Attachments.** This Agreement incorporates by way of attachment the following:

A. A list of all known business entity names related to the Requesting Party that will participate in the use and dissemination of the Data provided as Exhibit A;

B. The company policies provided to the Requesting Party's subscribers, customers, clients or other third parties as Exhibit B;

C. The original Request provided to the Division from the Requesting Party as Exhibit C; and

D. The approval letter provided to the Requesting Party from the Division as Exhibit D.

E. The Distribution Receipt Forms (Form TCM-AR9(F)-3).

These Exhibits may be amended or modified and are required to be updated by the Requesting Party in accordance with the terms of this Agreement. The amendments and or modifications shall be incorporated into this Agreement by reference on the attachments.

The undersigned individuals represent that they have the authority to execute this Agreement on behalf of their respective parties and execute this Agreement to be effective this ~~25th~~ 10th (JRW) day of ~~April, 2008~~ February, 2009. (JRW)

Requesting Party	Division
By: ~~Michael J Staresnick~~ Michael J Staresnick	By: Lilia Judson (JRW)
Printed: Michael J. Staresnick	Lilia Judson
Title: Estate Recovery Manager	Executive Director, Indiana Supreme Court Division of State Court Administration
Date: February 10, 2009 ~~April 25, 2008~~	Date: February 23, 2009

Exhibit A

KNOWN BUSINESS ENTITY NAMES

The Indiana Family and Social Services Administration

- Office of Medicaid Policy and Planning
- Division of Family Resources
- Division of Aging
- Division of Mental Health and Addictions
- Division of Disability and Rehabilitative Services
- Division of Technology Services

Exhibit B

COMPANY POLICIES

B.1. HIPPA Privacy Policy and Procedure Manual

B.2. HIPPA Security Policy and Procedure Manual

Family and Social Services Administration

Office of Medicaid Policy and Planning

HIPAA Privacy Policy and Procedure Manual

VERSION 6.4 (May 1, 2006)

Table of Contents

HIPAA

The *Health Insurance Portability and Accountability Act (HIPAA), Public Law 104-191*, was enacted on August 21, 1996. HIPAA contains three major provisions:

- Portability – Final rule published in 1997;
- Fraud and abuse/Medicare integrity program – Final rule published in 1998; and
- Administrative simplification – First final rule published August 17, 2000.

Administrative Simplification

The purpose of the administrative simplification provision is to improve health programs and the effectiveness and efficiency of the health care industry. This is accomplished by adopting common standards for health plans, health care clearinghouses, and health care providers that transmit or store any of the covered transactions provided in the *Standards for Electronic Transactions* final rule. As a health plan, the IHCP is required to comply with all HIPAA-related rules pertaining to:

- Administrative transactions,
- Unique identifiers,
- Code sets,
- Privacy, and
- Security.

Privacy

The IHCP, as a health plan, is required to comply with all requirements in the *Privacy Rule* as of April 14, 2003. The IHCP must have written policies, procedures, and safeguards in place, and all staff must be trained on these requirements.

Please note that business associates are responsible for compliance with the *Privacy Rule* for the functions contracted by the IHCP. This manual provides policies and procedures that the IHCP must comply with. For a complete definition of *business associate*, refer to the *Glossary* included in this manual.

The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) will be the enforcing agency for the *Privacy Rule*, to which a member can file a complaint if they believe that the IHCP is not protecting their information. Hereafter, the Secretary of the HHS will be referred to as the Secretary.

Overview

The *Family and Social Services Administration (FSSA), Office of Medicaid Policy and Planning (OMPP), HIPAA Privacy Policy and Procedure Manual* is designed to provide the FSSA/OMPP staff member with the policies and procedures necessary to comply with the *Health Insurance Portability and Accountability Act (HIPAA) Standards for Privacy of Individually Identifiable Health Information* final rule, published August 14, 2002.

Note: The Indiana Health Coverage Programs (IHCP) includes all OMPP programs and staff. All references to the IHCP within this manual also includes OMPP programs and staff.

Privacy Regulations

The Standards can be found in *45 Code of Federal Regulations* (CFR) *Parts 160 and 164*. Hereafter, the Standards will be known as the *Privacy Rule.*

Administration of Privacy Regulations

OMPP has established a privacy office for the IHCP to act as the gatekeeper of member protected health information (PHI), and most requests will be routed through this office.

EDS' Privacy Unit, as contracted by the OMPP, will function as the IHCP Privacy Office. Contact information for this office is as follows:

IHCP Privacy Office
P.O. Box 7260
Indianapolis, Indiana 46207-7260

The phone numbers for the IHCP Privacy Office are:
(317) 713-9627 or 1-800-457-4584

The IHCP Privacy Office point of contact for the OMPP staff is the OMPP Privacy Coordinator. The OMPP Privacy Coordinator will be responsible for ensuring that FSSA/OMPP staff members and contractors are in compliance with the *Privacy Rule.* Any questions regarding the *Privacy Rule* should be directed to the OMPP Privacy Coordinator. The current OMPP Privacy Coordinator is Jenifer Nelson, (317) 233-0446.

Administration of Privacy Regulations *(continued)*

The IHCP Privacy Office and the OMPP Privacy Coordinator, along with all members of the OMPP staff, under the auspices of FSSA's Privacy Official, are responsible for the overall compliance with the HIPAA rules and regulations relating to privacy of member's protected health information for the Indiana Health Care Programs. This includes Medicaid, the Children's Health Insurance Programs (CHIP), and 590 Program.

HIPAA Compliance: Role of OMPP Staff Members

In most cases, FSSA/OMPP staff members will refer requests for PHI to the IHCP Privacy Office. All written requests for member PHI will be submitted to the IHCP Privacy Office for processing, with the exception of requests related to TPL (which will continue to be handled by the EDS TPL Unit).

However, FSSA/OMPP staff members will continue to use and disclose PHI within the authorized, routine duties of their assigned positions. Staff members must be cognizant of the *Privacy Rule* in carrying out these authorized duties. This manual details appropriate procedures that each staff member must follow when using and/or disclosing PHI.

It is important that each staff member be aware of the requirements within the *Privacy Rule*, and of their obligation under the *Privacy Rule* to safeguard all PHI.

Any questions that FSSA/OMPP staff members may have regarding the *Privacy Rule* should be directed to the OMPP Privacy Coordinator.

Requirements of the IHCP

The *Privacy Rule* requires the Indiana Health Coverage Programs (IHCP), as a health plan, to provide protection and security to a member's protected health information (PHI) that is transmitted or maintained in any form, including oral communication.

What is Protected Health Information (PHI)?

A member's PHI includes the demographic information, recipient identification number (RID) number, and claim information (accounting or claim payment). For a complete definition of *protected health information*, refer to the *Glossary* included in this manual.

When can a member's PHI be released?

The policies and procedures contained within this manual will guide the FSSA/OMPP staff member in determining the steps to take when asked to provide a member's PHI to the member, the member's personal representative, or to another unit within FSSA, or another external agency or entity requesting the information.

In most units, the staff member will not provide any member PHI, but will refer the request on to the IHCP Privacy Office.

Use of PHI in daily work activities

The *Privacy Rule* also requires each staff member to be aware of the PHI that they use in their daily work activities. Not only must the staff member protect the member's information in regard to requests, but also in their work functions and work environment. The *Privacy Rule* requirements establish specific administrative, technical, and physical safeguards. These safeguards cover such common activities as conversation's regarding a member's PHI, the access of a member's PHI, the copying and faxing of PHI, and the proper disposal of PHI documents.

NOTE: The policies and procedures contained within this manual are not intended to prevent staff members from using and disclosing PHI within the authorized, routine duties of their assigned positions. The procedures OMPP staff must follow when carrying out these authorized duties are detailed throughout the appropriate sections of this manual. Appendix G of this manual provides a "quick reference guide" of procedures to be followed by staff members when using and disclosing PHI in their daily work activities.

IHCP Member Rights

As provided in the final *Privacy Rule*, the member has the right of assurance that his or her health information is secure and is used by the FSSA/OMPP staff, including contractor staff such as EDS, in the appropriate and most secure manner possible, as required by the *Privacy Rule*. Each staff member is responsible for safeguarding the member's PHI in his or her daily work and work environment.

Document Organization

This manual contains the following information for the employee's reference and use when a question arises regarding the use or disclosure of a member's PHI:

- Privacy policy and procedure sections, containing:
  - The purpose of the section,
  - The IHCP-specific policy, and
  - The IHCP-specific procedure.
- Glossary explaining terms in relation to the HIPAA *Privacy Rule*.
- Appendices A-F containing forms and notices referenced in this manual.
- Appendix G containing a "quick reference guide" for FSSA/OMPP staff on their roles in handling PHI uses and disclosures.

Note: Where appropriate, Code of Federal Regulations (CFR) citation(s) are provided. For additional information regarding the policy and procedures, refer to the CFR.

Most common policy and procedure documents

The specific privacy policy and procedure documents that will be referenced most commonly by employees are categorized as follows:

- *Notice of Privacy Practices*,
- Uses and disclosures of protected health information,
- Minimum necessary requirements,
- Uses and disclosures of protected health information when member authorization is not required,
- Member rights, and
- Privacy of PHI information requirements to be followed by all FSSA/OMPP staff.

Definitions

For a complete listing of definitions associated with the *Privacy Rule*, refer to the *Glossary* included in this manual.

Summary

HIPAA rules and regulations

On August 21, 1996, the Health Insurance Portability and Accountability Act, commonly known as HIPAA, was signed into law. As its name implies, HIPAA included a number of provisions to make health coverage more portable for employees changing jobs by limiting exclusions for pre-existing conditions. In addition, HIPAA also included a set of "Administrative Simplification" provisions, which were intended to improve the efficiency and effectiveness of the health care system.

In drafting HIPAA, Congress recognized the threats to confidentiality posed by the growing complexity of the health care system and the increased used of electronic data interchange that HIPAA itself was intended to encourage. Thus, the Administrative Simplification provisions of HIPAA authorized the U.S. Department of Health and Human Services (HHS) to issue standards for the privacy of individually identifiable health information if Congress failed to enact health care privacy legislation by August 21, 1999. Congress failed to meet this self-imposed deadline, and HHS published proposed regulations on November 3, 1999. The Department reviewed more than 52,000 comments in response to the proposed rule and published a final rule shortly before the end of the Clinton administration. The Bush administration published a revised final rule, referred to as the *Privacy Rule*, on August 14, 2002.

Purpose of this manual

This manual is a resource provided to assist OMPP staff members in interpreting the *Privacy Rule*. Key components of the *Privacy Rule* are presented in sections. Policies and procedures, specific to the IHCP, are provided in each section.

It is important for all OMPP staff to be knowledgeable of the *Privacy Rule,* as presented in this manual, in addition to the policies and procedures specific to the IHCP, to ensure compliance with HIPAA rules and regulations.

Questions or concerns relating to privacy

Any questions that FSSA/OMPP staff may have regarding the contents of this manual, or questions relating to privacy, will be directed to the OMPP Privacy Coordinator.

If you have any concerns or doubts about your authority to use or disclose any IHCP PHI, contact the OMPP Privacy Coordinator for clarification.

If you believe any FSSA/OMPP staff members or contractors are using or disclosing PHI inappropriately, either intentionally or unintentionally, please notify the OMPP Privacy Coordinator.

Section 2: Notice of Privacy Practices

Purpose

To issue instructions to all FSSA/OMPP staff and IHCP contractor staff regarding the policy for the creation, revision, and mailing of the *Notice of Privacy Practices* to IHCP members.

Policy

The IHCP is responsible for issuing a *Notice of Privacy Practices* (NPP) document to IHCP members, which provides notice of the uses and disclosures of PHI that may be made by the IHCP, of the member's rights, and of the IHCP legal duties with respect to PHI.

The *Notice of Privacy Practices* document (Appendix A) contains the information that the IHCP is required to provide to each IHCP member pursuant to 45 CFR 164.520.

Initial Mailing of the Notice of Privacy Practices

The first *Notice of Privacy Practices* will have been mailed to all current IHCP members in April 2003, prior to the HIPAA *Privacy Rule* compliance date of April 14, 2003. The members' enrollment status will be determined at the time of the notice print date. This date will be used, in the future, as the date to determine if a member has received the required notice.

Posting of NPP on Web Site

The notice will be maintained on the http://www.in.gov/fssa/servicedisabl/medicaid/medprivacy.html Web site and will be provided upon request to any member except for correctional facility inmates, who do not have a right to notice.

Deleted: www.indianamedicaid.com

Mailing of NPP to new members

After the initial mailing of the notice, all new members will receive the *Notice of Privacy Practices* document with their new IHCP RID identification card. For IHCP members who do not receive an automatic mailing of the IHCP RID identification card, a separate notice mailing will occur upon the member's enrollment in one of the following IHCP programs or aid categories:

- 590 Program
- Special Low Income Medicare Beneficiary (SLIMB)
- Qualified Individual –1 (QI-1)
- Qualified Disabled Working Individual (QDWI)
- Qualified Medicare Beneficiary (QMB)

For these five groups, a 'notice only' file will be created within Indiana*AIM,* which will generate the notice mailing process outside of the IHCP RID card creation process.

Subsequent mailings of the NPP

The IHCP will notify covered members of the availability of the notice and how to obtain the notice, no less frequently then once every three years. Therefore, the next scheduled time for release of this notice to members was April of 2006.

Deleted: will be

Revisions to the Notice of Privacy Practices

The IHCP will provide a revised *Notice of Privacy Practices* document to members within 60 days of a material revision to the notice, if applicable.

Procedure

NPP Mailing

The fiscal agent will mail the NPP to all new members upon their enrollment in the IHCP, and to all members within 60 days of any material change to the notice. Members received an initial mailing during April of 2003.

After the initial mailing, the IHCP will notify covered members of the availability of the NPP at least every 3 years.

Web Site

The NPP will be maintained on the http://www.in.gov/fssa/servicedisabl/medicaid/medprivacy.html Web site.

Deleted: www.indianamedicaid.com

Questions

Any requests for additional copies of the NPP, or questions related to the NPP, should be referred to the IHCP Privacy Office at the fiscal agent.

The address for the IHCP Privacy Office is:

IHCP Privacy Office
P.O. Box 7260
Indianapolis, Indiana 46207-7260

The phone number is: (317) 713-9627 or 1-800-457-4584

Deleted: 488-5018

NPP Document

The *Notice of Privacy Practices* document, as mailed to all IHCP members, is shown in Appendix A.

Section 3: Permitted and Required Uses and Disclosures of Protected Health Information

Purpose

To issue instructions to all FSSA/OMPP staff regarding the policy and procedures for permitted uses and disclosures of PHI.

Policy

Use of PHI for Treatment, Payment, and Health Care Operations (TPO)

The IHCP is allowed to use or disclose PHI, to the extent permitted by the *Privacy Rule*.

The IHCP must document (i.e., account for) all instances in which PHI is released to an external entity for purposes other than treatment, payment, or health care operations, since an IHCP member has the right to request and receive an accounting for such disclosures (please refer to Section 18 of this manual, *Accounting of Disclosures to Member*, for further explanation).

For a complete definition of *treatment, payment, and healthcare operations (TPO)*, refer to the *Glossary* included in this manual.

The majority of PHI received and disclosed by the IHCP is used for treatment, payment, and healthcare operations (TPO), so the disclosure of PHI for other purposes should be minimal.

Accounting of Disclosures to Members

The *Accounting of Disclosures to Member* section (Section 18 in this manual) should be referenced to determine which disclosures the IHCP must account for, and what information must be documented and maintained in order to provide an accounting of disclosures to members upon request by a member.

Permitted Uses and Disclosures

The IHCP may use or disclose PHI:

- To the member;
- For treatment, payment, or healthcare operations (TPO);
- As permitted by, and in compliance with, the following situations:
  - Uses and disclosures required by law;
  - For public health activities, if required by law;
  - Health oversight agency;
  - Judicial proceedings;
  - Research (for a related State Plan purpose); and
  - Law enforcement purposes; or
- Pursuant to an authorization or agreement by the member.

Required Disclosures of PHI

The IHCP is required to disclose protected health information:

- To a member or to a member's personal representative, when requested under, and as required by the *Privacy Rule*, or
- When required by the Secretary of HHS to investigate or determine the IHCP compliance with the *Privacy Rule*.

Routine uses or disclosures

A *routine use or disclosure* is one of a series of repetitive uses or disclosures:

- Which are made to the same person or entity, pursuant to a single authorization and
- Which are for the same purpose, pursuant to a single authorization; or
- Which are permitted without authorization under the *Privacy Rule,* for the purposes of treatment, payment, or healthcare operations.

All routine use or disclosure requests that require authorization will be forwarded to the IHCP Privacy Office, who will then complete the request and document the recurring PHI use or disclosure.

The uses and disclosures must be documented according to the *Accounting of Disclosures to Member* Section 18, as appropriate.

Non-routine uses or disclosures

A *non-routine use or disclosure* is a unique, one-time request made by a person or entity for the use or disclosure of PHI pursuant to an authorization, or as permitted without authorization under the *Privacy Rule* (i.e., not for the purpose of treatment, payment, or healthcare operations).

All non-routine use or disclosure requests that require authorization will be forwarded to the IHCP Privacy Office, who will then complete the request and document the PHI use or disclosure.

Some requests might be denied.

If release of the PHI is approved, the Privacy Office will coordinate the requested release with the appropriate EDS Unit, OMPP Unit, or HCE Unit.

The uses and disclosures will be documented as found in the *Accounting of Disclosures to Member* Section 18, as appropriate.

Minimum Necessary Requirement

When using or disclosing PHI, the IHCP must:

- Provide only the minimum necessary PHI to accomplish the intended purpose of the use, disclosure, or request (for additional information, see Section 4, Minimum Necessary Requirements, of this manual); and
- Have appropriate administrative, technical, and physical safeguards in place to protect the member's PHI (for additional information, see Section 20, *Protected Health Information Safeguards*, of this manual).

Procedure

Disclosure of PHI for TPO

OMPP staff members will continue to use and disclose PHI within the authorized, routine duties of their assigned positions. For example, if an individual calls a staff member with a simple request, but one which would require the staff member to release PHI to that individual, the staff member may still directly respond to this individual after following the proper protocols to verify the identity and authority of the requesting individual.

Specific disclosure requirements and protocols are provided Appendix G of this manual.

Disclosure of PHI for purposes other than for TPO

PHI will **not be used or disclosed for any purposes** other than treatment, payment, and healthcare operations (TPO), without the express approval of the OMPP Privacy Coordinator.

PHI disclosure requests which are outside the authority of OMPP staff members, should be forwarded to the IHCP Privacy Office:

IHCP Privacy Office
P.O. Box 7260
Indianapolis, Indiana 46207-7260

The phone number is: (317) 713-9627 or 1-800-457-4584

Deleted: 488-5018

Definition of TPO

See the *Glossary* included in this manual for a detailed definition of TPO.

Regulatory Requirements and Authority: 45 CFR 164.502

Section 4: Minimum Necessary Requirements

Purpose

To issue instructions to all FSSA/OMPP staff regarding the policy and procedures relating to the minimum necessary requirements for the use and disclosure of PHI.

This section pertains specifically to the use and disclosure of PHI information outside of the IHCP.

Refer to the *Protected Health Information Access for Staff Use*, Section 19 of this manual, for further detail regarding the minimum necessary requirements for FSSA/OMPP staff.

Policy

Minimum Necessary Requirement

For most PHI uses and disclosures, the IHCP must apply the minimum necessary requirements. The IHCP shall limit access and use of PHI by its staff and contractors to the minimum necessary to accomplish the defined work functions. The requirements also apply to PHI requests made by, or on behalf of, the IHCP to another covered entity.

Types of information for which access limitations apply

The access limitations apply to electronic, paper, and oral communication of PHI. This is inclusive of Indiana*AIM*, OnDemand, and Business Objects access, along with any other database or repository of information containing PHI.

Exclusions to the Minimum Necessary Requirement

There are instances in which the minimum necessary limitation is **not required**, including:

- Disclosures made to a member's health care provider for the purpose of providing treatment;
- Disclosures made to the member or through the member's written authorization in regard to their own PHI; or
- Uses or disclosures required by law, and when required by the Secretary of HHS to investigate or determine IHCP compliance with the *Privacy Rule*.

Procedure

Limited access by FSSA/OMPP staff	FSSA/OMPP staff will have access to the minimal amount of member PHI that is necessary to perform required work functions. The appropriate unit supervisor will be responsible for determining access needed for assigned staff members, and for granting the appropriate access to assigned staff members. Documentation regarding such access will be maintained by the OMPP Privacy Coordinator.
Disclosure of PHI for TPO	OMPP staff members will continue to use and disclose PHI within the authorized, routine duties of their assigned positions. PHI used for such authorized purposes will be limited to the minimum necessary to accomplish the defined work functions. Refer to Table 4.1 on the following page for a summary of specific disclosures (including disclosure of TPO) that must be limited to the minimum necessary.
Disclosure of PHI for purposes other than for TPO	PHI will **not be used or disclosed for any purposes** other than treatment, payment, and healthcare operations (TPO), without the express approval of the OMPP Privacy Coordinator. Use or disclosure of PHI will then be limited to the minimum necessary to accomplish the defined work functions.
Definition of TPO	See the *Glossary* included in this manual for a detailed definition of TPO.

Regulatory Requirements and Authority:
45 CFR 164.502(b) and 164.514(d)

Table 4.1: Protected Health Information – Summary of Minimum Necessary Requirements

PHI release requested to/for:	Minimum Necessary Standard Applies
To a member	No- after verification of identity
To a member's personal representative/legal guardian	No- after verification of identity
To a member's health care provider*	No- after verification of identity
To a member's attorney	No- after authorization
To a member's legislative representative	No- after authorization
To a deceased member's personal representative	No- after verification of identity/authorization
For payment purposes*	Yes
For health care operation purposes*	Yes
Required by law	PHI release must be limited to the relevant requirements of the specific law.
For public health activities	PHI release must be limited to the relevant requirements of the specific law.
For law enforcement purposes	Yes
For health oversight activities	Yes
For worker's compensation activities	Yes
To the Secretary of HHS	No
De-identified information	Individually identifiable information is removed before disclosure.
Limited data set	May only be used for research, public health, or health care operation purposes, select direct identifiers are removed from information before disclosure.
By a whistleblower	Yes
By a workforce crime victim	Limited to the requirements in 45 CFR 164.502(j)
Prior to April 14, 2003	No

Deleted: No

Deleted: No

Deleted: No

* Psychotherapy notes can be disclosed without member authorization ONLY for the following specific treatment, payment, and health care operations:

- Use by the originator of the psychotherapy notes for treatment
- Use or disclosure by the IHCP to defend itself in a legal action or proceeding brought by the member
- A use or disclosure permitted with respect to the oversight of the health care provider originating the psychotherapy notes.
- For any other use, coordinate with the OMPP Privacy Coordinator.

Section 5: De-identified Protected Health Information

Purpose

To issue instructions to all FSSA/OMPP staff regarding the policy and procedures relating to the de-identification of PHI and the use of de-identified PHI.

Policy

De-identified information and PHI requirements

Health information that meets the standards for de-identified PHI is not considered to be individually identifiable information. The requirements for PHI use and disclosure do not apply to de-identified PHI if the requirements for de-identifying the information have been met and the disclosure of a code or other means of re-identification have not been disclosed to the de-identified information requester.

Definition of de-identified information

The IHCP is permitted to use PHI to create information that does not individually identify members. De-identified PHI is information where the removal of data elements has made the identification of a member impossible from the data contained on a released document, released dataset, or disclosed orally.

Limited Data Set

PHI that excludes specific direct identifiers of the individual or of relatives, employers, or household members of the individual constitutes a limited data set. A limited data set is considered de-identified PHI and therefore not considered to be individually identifiable information. See *IHCP Limited Data Set*, in the Glossary Section of this manual, for a complete description of a limited data set, as applicable to the IHCP.

Requirements of de-identified PHI

The IHCP may determine that health information is de-identified PHI only if:

- A person with appropriate knowledge of and experience with generally accepted statistical and scientific principals and methods renders the information individually de-identified; **AND**
- The following identifiers of the member or of relatives, employers or household members of the individual are removed (limited data set):
  - Names;
  - All geographic subdivisions smaller than a State, including street address, city, county (except as noted below*), precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if the geographical unit formed by the zip code contains more than 20,000 people;
  - All elements of dates (except year) for dates directly related to member, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
  - Telephone numbers;
  - Fax numbers;
  - Electronic mail addresses;
  - Social security numbers;
  - Medical record numbers;
  - Health plan beneficiary numbers;
  - Account numbers;
  - Certificate/license numbers;
  - Vehicle identifiers and serial numbers, including license plate numbers;
  - Device identifiers and serial numbers;
  - Web Universal Resource Locators (URLs);
  - Internet Protocol (IP) address numbers;
  - Biometric identifiers, including finger and voice prints;
  - Full face photographic images and any comparable images; and
  - Any other unique identifying number, characteristic, or code; and the covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is subject of the information.

Requirements of de-identified PHI *(continued)*

* **NOTE**

In counties or any other geographic subdivisions with populations less than 20,000 (this could be a city, zip code, precinct, etc.), the geographic identifier must be removed. If County X and County Y each have populations of less than 20,000, then these county codes must be removed, in addition to other identifying information as detailed above, in order for the data set to be considered limited. However, if County Z has a population of 50,000, then the county identifier may be provided and the data set would still be considered a limited data set.

Permitted use and disclosure of de-identified PHI

The IHCP is permitted to use de-identified PHI and can release de-identified information without the member's consent.

Accounting of disclosures

The IHCP is not required to account (i.e., document) for the disclosure of de-identified PHI to the member.

Re-identification of otherwise de-identified PHI

Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of PHI.

If de-identified information is re-identified, the IHCP may use or disclose such re-identified information only as permitted or required by the *Privacy Rule*.

Procedure

Who will de-identify PHI	Only FSSA/OMPP staff designated by the OMPP Privacy Coordinator will perform the de-identification process for PHI.
De-identification for routine releases	Key staff, designated by the OMPP Privacy Coordinator, will be responsible for verifying that PHI has been properly de-identified. This needs to be done only the initial time for routine reports or releases (for example, a report produced each quarter for entity X, would only need to be verified one time, prior to the initial release, and does not need to be verified prior to each quarterly release UNLESS changes are made to the report content).
De-identification for non-routine releases	For non-routine reports or releases, the key staff member(s) identified by the OMPP Privacy Coordinator will verify each time that the PHI had been properly de-identified prior to release of information to any person or entity (for example, a single report requested by entity X, that is not a standard report produced for release, would be classified as a non-routine report and would therefore require verification prior to release)

Regulatory Requirements and Authority:
45 CFR 164.502(d) and 164.514(a)-(c)

Section 6: Disclosures to Business Associates

Purpose

To issue instructions to all FSSA/OMPP staff regarding the policy and procedures for permitted uses and disclosures of PHI to their business associates.

Policy

Business Associates (defined)

A person or organization that performs a function or activity on behalf of the IHCP, but is not part of the FSSA/OMPP staff, such as EDS, Health Care Excel (HCE), or Myers and Stauffer.

Use of a business associate

The IHCP contracts with numerous business associates to carry out functions on behalf of the IHCP. The IHCP uses business associates to arrange, perform, or assist in the performance of a function or activity involving the use or disclosure of PHI, including claims processing, and health care operations, on the behalf of the IHCP.

Disclosures to Business Associates

Before the IHCP may disclose PHI to a business associate or allow a business associate to create or receive PHI on behalf of the IHCP, the IHCP must obtain satisfactory assurance in the form of a written business associate agreement, or contract amendment containing terms of a business associate agreement. The terms of the business associate contract or amendment must specify that the business associate will appropriately safeguard and limit the use and disclosure of PHI to the minimum necessary to fulfill their contractual requirements.

Business Associate Agreement

The language in the business associate agreement requires the business associate to adhere to all federal and state laws and statutes for the privacy of PHI.

Breach or Violation by a business associate

If the IHCP learns that a business associate has materially breached or violated the satisfactory assurance of its business associate contract, the IHCP must take prompt, reasonable steps to see that the breach or violation is cured. If the business associate does not promptly and effectively cure the breach or violation, the IHCP must terminate the contract with the business associate, or if contract termination is not feasible, report the business associate's breach or violation to Health and Human Services.

Exclusions

This standard does not apply:

- With respect to disclosures by the IHCP to a health care provider concerning the treatment of a member; or
- With respect to uses or disclosures by the IHCP, county caseworkers, and staff who maintain the Indiana Client Eligibility System (ICES) as they relate to the determination of member eligibility and enrollment in the IHCP.
- Neither providers nor the local office of Family and Children are considered "business associates" under HIPAA.

Procedure

Releasing PHI to business associates

Business associates may require PHI to effectively perform contracted functions of the IHCP. PHI may be disclosed to business associates only to perform authorized functions **as specified in the approved business associate agreement.**

Questions

Any questions regarding release of PHI to business associates should be addressed to the OMPP Privacy Coordinator.

Suspected breach or violation	The OMPP Privacy Coordinator should be notified immediately if a business associate is suspected of breaching or violating their business associate agreement. The OMPP Privacy Coordinator will document and investigate the suspected breach or violation. If a violation or a breach has occurred the business associate will be given an opportunity to cure the breach or violation.
Verified breach or violation	If the business associate does not promptly and effectively cure the breach or violation, the IHCP will terminate the contract with the business associate.
Mitigation	The IHCP must mitigate, to the extent practicable, any harmful effect that is known to the IHCP of a use or disclosure of protected health information in violation of policies and procedures, or of any requirements contained within the *Privacy Rule*, by a business associate.

Regulatory Requirements and Authority: 45 CFR 164.502(e)

Section 7: Protected Health Information of Deceased Members

Purpose

To issue instructions to all FSSA/OMPP staff regarding the policy and procedures for acceptance of, response to, and documentation of requests for PHI of deceased members.

Policy

Rights of personal representative

The IHCP must allow the personal representative of the deceased member the right to inspect or copy the member's PHI contained in the designated record set (for a complete definition of *designated record set*, refer to the *Glossary* included in this manual). Notice of these rights and the process for the member's personal representative to follow in order to exercise them are provided to each IHCP member in the *Notice of Privacy Practices.*

The IHCP is allowed to use or disclose PHI of a deceased member to a personal representative who is permitted under applicable law to act with respect to the interest of the deceased or on behalf of the deceased's estate or to make decisions regarding the deceased member's PHI. Proof of the representative's identity and authority must be provided prior to the release. See Appendix C for the *Verification of Identity and Authority Form.*

Requests for access to records by the personal representative

The IHCP will require that the personal representative of the deceased member make the request in writing. All requests for access received by the IHCP Privacy Office will be documented, reviewed, and responded to the requesting personal representative of the deceased member by the IHCP Privacy Office, within the timeframes required by the *Privacy Rule.*

Requirement to protect PHI of deceased members	The IHCP must comply with the PHI requirements of the *Privacy Rule* with respect to the PHI of a deceased member. The IHCP is required to protect PHI about deceased members for as long as it maintains the information.
When the IHCP is not the originator of the PHI	In most cases of PHI, the IHCP is not the originator of the information. In cases where IHCP is not the originator, the IHCP will refer the member to the healthcare provider originating the PHI.
Accounting of disclosures	The accounting of disclosures for a deceased member's PHI is treated like that for a living member's PHI, including the exceptions as noted in the *Accounting of Disclosures to Member* Section 18. The decedent's personal representative has the right to request and receive the disclosure accounting. The IHCP Privacy Office will manage all requests for disclosure accountings.

Procedure

Requests for PHI for deceased member	The IHCP Privacy Office will manage all requests for copies of PHI from deceased member's authorized personal representatives, with the exception of those requests related to Medicaid estate recovery. This includes requests for copies of PHI that may be maintained by FSSA/OMPP staff. If a deceased member's representative requests a copy of their PHI, refer them to the IHCP Privacy Office. IHCP Privacy Office P.O. Box 7260 Indianapolis, Indiana 46207-7260 The phone number is: (317) 713-9627 or 1-800-457-4584 The IHCP Privacy Office will be responsible for verification of the individual requesting information on behalf of a deceased member.

Deleted: 488-5018

Regulatory Requirements and Authority:
45 CFR 164.502(f) and 164.512(g)

Section 8: Disclosures to Personal Representatives and Rights of Minors

Purpose

To issue instructions to all FSSA/OMPP staff regarding the policy and procedures for disclosures of PHI to a member's personal representative and the rights of a minor.

Policy

Rights of the Personal Representative

A designated personal representative of a member has the right to inspect and obtain a copy of the member's PHI in the IHCP designated record set. The IHCP must treat a personal representative as the member with respect to PHI, except as indicated in the *Privacy Rule* for unemancipated minors (as defined in the *Glossary*), and in situations of abuse, neglect, and endangerment.

See Appendix I to access the *Personal Representative Authorization Form*, which is used to designate a member's personal representative.

Requests for PHI by a Personal Representative

The IHCP will require the personal representative to complete a written request using the *Member Access Request* form (see Appendix B). The personal representative must provide a copy of documentation supporting representation of the member. All written requests for access received by the IHCP Privacy Office will be documented, reviewed, and responded to by the IHCP Privacy Office, within the timeframes required by the *Privacy Rule*.

When the IHCP is not the originator of the PHI

In most cases of PHI, the IHCP is not the originator of the information. In this case, the IHCP will refer the personal representative to the healthcare provider originating the PHI.

Unemancipated Minors

In the state of Indiana, a parent, guardian, or other court appointed representative is entitled to exercise the member's rights on the member's behalf if the member is an unemancipated minor. The IHCP must treat such individuals as personal representatives of members who are unemancipated minors, with respect to PHI.

Parental Rights

A custodial parent and noncustodial parent of a child have equal access to the child's health records unless:

- A court has issued an order that limits the noncustodial parent access to the child's health records; and
- The IHCP has received a copy of the court order; or
- The IHCP has actual knowledge of the final court order.

Adults and Emancipated Minors

If under state law a person has authority to act on behalf of a member who is an adult or an emancipated minor in making decisions related to health care, the IHCP must treat such person as a personal representative with respect to PHI.

Revocation of rights as a personal representative

The IHCP may decide not to treat a person as the personal representative of a member if the IHCP has a reasonable belief that:

- The member has been or may be subjected to domestic violence, abuse, or neglect by such person; or
- Treating such person as the personal representative could endanger the member; and
- The IHCP, in the exercise of professional judgment, decides that it is not in the best interest of the member to treat the person as the member's personal representative.

Procedure

Requests for PHI from Personal Representatives

The IHCP Privacy Office will manage all requests for copies of PHI from personal representatives of members. This includes requests for copies of PHI that may be maintained by FSSA/OMPP staff.

If a personal representative of a member requests a copy of their PHI refer them to the ICHP Privacy Office.

IHCP Privacy Office
P.O. Box 7260
Indianapolis, Indiana 46207-7260

The phone number for the IHCP Privacy Office is: (317) 713-9627 or 1-800-457-4584

Deleted: 488-5018

The IHCP Privacy Office will be responsible for verification of the individual requesting information on behalf of a member.

Regulatory Requirements and Authority:
45 CFR 164.502(g) and
Indiana Code (IC) 16-39-1-3 and IC 16-39-1-1

Section 9: Disclosures by Whistleblowers

Purpose

To issue instructions to all FSSA/OMPP staff regarding the policy and procedures relating to PHI disclosures by whistleblowers and workforce member crime victims.

Policy

Disclosures by Whistleblowers

A workforce member or business associate of the IHCP has the right to disclose PHI if they believe in good faith that the IHCP has engaged in conduct that is unlawful or otherwise violates professional standards, or that the services or conditions provided by the IHCP endangers one or more members, workers, or the public. The IHCP will not be considered to have violated the requirement of the *Privacy Rule* if a member of its workforce or a business associate discloses PHI, provided that the disclosure is made to:

- A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the IHCP or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the IHCP, or
- An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct of the IHCP.

Disclosures by Workforce Members

A workforce member who is a victim of a criminal act has the right to disclose PHI information to law enforcement officials. The IHCP, or its business associates, will not be considered to have violated the requirements of the *Privacy Rule* if a member of it's workforce who is a victim of a criminal act discloses PHI information to a law enforcement official to be used for purposes to identify and locate a suspected perpetrator, provided that:

- The PHI disclosure is about the suspected perpetrator of the criminal

act; and

Disclosures by Workforce Members *(continued)*

- The PHI disclosed is limited to the information listed below:
  - Name and address;
  - Date and place of birth;
  - Social Security Number;
  - Type of injury;
  - Date and time of treatment; and
  - Date and time of death, if applicable.

Procedure

Accounting of disclosures

The IHCP is not required to account for disclosures, to the IHCP member, by whistleblowers and workforce member crime victims. See the *Permitted and Required Uses and Disclosures of Protected Health Information* Section 3 for additional information.

Regulatory Requirements and Authority:
45 CFR 164.502(j)

Section 10: Uses and Disclosures of Protected Health Information When Member Authorization is Not Required

Purpose

To issue instructions to all FSSA/OMPP staff regarding the policy and procedures relating to uses and disclosures of PHI that does not require a member's authorization.

The *Privacy Rule* allows a covered entity to provide PHI without an individual's authorization for various reasons; however, given the IHCP status as a health plan as opposed to a direct provider of healthcare, the IHCP will have limited circumstances when these requirements are applicable. The full extent of the requirements can be found at 45 CFR 164.512 (a)-(l).

The IHCP scope of activity is documented in the *Policy* and *Procedure* discussions immediately following.

Policy

Use of a member's PHI

The IHCP may use or disclose a member's PHI without their written authorization or without providing the member the opportunity to object to the use or disclosure for the purposes of treatment, payment, and health care operations (TPO).

There are some situations in which the IHCP is required to notify the member of the PHI use or disclosure, and some in which the member can agree to the use or disclosure. In these situations, the IHCP may provide notification verbally to the member and then the member can give agreement verbally.

Permitted disclosure of PHI without written authorization

Although the *Privacy Rule* provides for many instances in which the IHCP can use or disclose PHI without a member's written authorization, there are limited circumstances when this will occur within the IHCP. Common situations within the IHCP that do not require written authorization for disclosure of PHI include:

- Uses and disclosures for the purposes of treatment, payment, or health care operations;
- Uses and disclosures required by law, including:
  - Court orders and court-ordered warrants;
  - Subpoenas or summons issued by a court, grand jury, or inspector general; or
  - A civil or an authorized investigative demand;
- Uses and disclosures for public health activities if required by law;
- Uses and disclosures for health oversight activities, including:
  - Civil, criminal, or administrative investigations;
  - Audits or inspections; or
  - An investigation or activity that comes from or is directly related to the receipt of health care, a claim for public benefits related to health, or qualification for, or receipt of, public benefits or services related to a member's health;
- Disclosures for judicial and administrative proceedings, as described under uses and disclosures required by law;
- Disclosures for law enforcement purposes, as described under uses and disclosures required by law;
- Disclosures for workers' compensation for purposes of TPL or similar programs as established by law;
- Disclosures of PHI to an attorney for the purpose of third party liability (TPL) settlement.

Minimum Necessary Requirement

With the exception of uses or disclosures that are required by law, the IHCP must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request for the purposes described above. See Section 4 of this manual, *Minimum Necessary Requirements*, for additional information on this topic.

Verification and documentation requirements

Note: The IHCP must verify the identity of the person requesting PHI, and whether the person has the authority to access PHI, if the identity or such authority of the person is not known to the IHCP. Also, the IHCP must obtain any documentation, statements, or representations (written or oral) from the person requesting the PHI when the documentation, statement, or representation is required for the PHI disclosure (see Section 12, and Figure 12.1). The IHCP Privacy Office will be responsible for those disclosures requiring verification and documentation.

Accounting of Disclosures

Uses and disclosures of PHI will be documented, as required by the *Privacy Rule*, for the purpose of providing an *Accounting of Disclosures* to members. See Section 18 of this manual, *Accounting of Disclosures to Member*, for specific uses and disclosures for which an accounting is required, and for additional information regarding this topic.

IHCP members may request an *Accounting of Disclosures*, except for those cases where the member's rights for such an accounting are suspended. These cases would involve:

- National security and intelligence activities or
- Correctional institutions and other law enforcement custodial situations.

Requests for PHI use or disclosure

All requests for PHI use or disclosure discussed in this section must be referred to the IHCP Privacy Office, with the exception of requests for PHI disclosures related to workers' compensation or similar programs as established by law, and for disclosures for TPO within the IHCP. Requests for disclosures related to workers' compensation or similar programs are directed to, and will be responded to by, the IHCP Third Party Liability (TPL) Unit. Disclosures of PHI for the purposes of TPO do not require tracking or approval.

Procedure

PHI will not be used or disclosed for any purposes other than treatment, payment, and healthcare operations (TPO), without the express approval of the OMPP Privacy Coordinator.

See the *Glossary* included in this manual for a detailed definition of TPO.

Regulatory Requirements and Authority: 45 CFR 164.512(a)-(1)

Section 11: IHCP Member Access to Protected Health Information

Purpose

To issue instructions to all FSSA/OMPP staff regarding the policy and procedures relating to members' rights relating to their access to PHI.

Policy

Member Rights

A member, or a designated personal representative of the member, has the right to inspect and obtain a copy of their PHI in the IHCP designated record set. The IHCP must allow the member the right to inspect or copy their PHI, which is contained in the designated record set. Notice of these rights and the process for the member to follow to exercise them are provided to each IHCP member in the *Notice of Privacy Practices.*

Requests for access to PHI

The IHCP requires that the member, or the member's personal representative, make the request in writing. All written requests for access received from a member or the member's personal representative, will be documented, reviewed, and responded to, by the IHCP Privacy Office, within the timeframes required by the *Privacy Rule.*

When the IHCP does not maintain the PHI

For some cases, the IHCP does not maintain the requested PHI (i.e., medical records are originated and maintained by a physician or hospital). In this case, the IHCP will refer the member to the healthcare provider maintaining the PHI.

Accounting of disclosures

A use or disclosure of PHI requested by the member, or the member's personal representative, is not required to be included in the accounting of disclosures of that member's PHI.

Procedure

Requests for PHI

In most cases, the IHCP Privacy Office will manage all requests for copies of PHI from members. This includes requests for copies of PHI that may be maintained by FSSA/OMPP staff.

However, this procedure is not intended to impede usual operational protocols. Authorized staff members may continue to use and disclose PHI within the authorized, routine duties of their assigned positions. Appropriate procedures to follow when carrying out these authorized duties are detailed throughout the appropriate sections of this manual, and in Appendix G.

If a member requests a copy of their PHI, refer them to the IHCP Privacy Office as appropriate.

IHCP Privacy Office
P.O. Box 7260
Indianapolis, Indiana 46207-7260

The phone number is: (317) 713-9627 or 1-800-457-4584

Deleted: 488-5018

Regulatory Requirements and Authority: 45 CFR 164.524

Section 12: Verification of Identity and Authority

Purpose

To issue instructions to all FSSA/OMPP staff regarding the policy and procedures relating to the identity and authority verification of the person requesting PHI and the documentation required to substantiate the PHI disclosure request.

Policy

Identification of person requesting PHI

The IHCP must verify the identity of the person requesting PHI, and whether the person has the authority to access PHI, if the identity or such authority of the person is not known to the IHCP. Also, the IHCP must obtain any documentation, statements, or representations (written or oral) from the person requesting the PHI when the documentation, statement, or representation is required for the PHI disclosure. The IHCP Privacy Office will be responsible for those disclosures requiring verification and documentation.

Member Requests for Access to PHI

Some member requests for access to PHI will be forwarded to the IHCP Privacy Office for response. The IHCP Privacy Office will handle all written requests.

However, some requests from members will be handled directly by FSSA/OMPP staff members.

Staff members must follow required protocols prior to releasing any PHI to members. See Appendix G for protocols.

Verification

The IHCP will continue to verify the identity of a member who is requesting the use or disclosure of his or her own PHI.

Accounting of Disclosures

If a member requests an accounting of disclosures of their PHI made by the IHCP, any prior disclosure made at the member's request are not required to be documented in this accounting.

Note: Please refer to Section 11 of this manual, *IHCP Member Access to Protected Health Information,* for specific details.

Member's Personal Representative Requesting PHI Access

Some member personal representative requests for access to PHI will be forwarded to the IHCP Privacy Office for response. The IHCP Privacy Office will handle all written requests.

However, some requests will be handled directly by FSSA/OMPP staff members.

Staff members must follow required protocols prior to releasing any PHI to a member or their personal representative. See Appendix G for protocols, and Appendix I for the *Personal Representative Authorization Form.*

Verification

A member's personal representative or legal guardian must provide documentation verifying their authority to request the member's PHI, and must be authorized to act as the member's personal representative. See Appendix I for the *Personal Representative Authorization Form.*

For PHI requests initiated by a member's personal representative, the *Verification of Identity and Authority* form will be used to verify identity (see Appendix C). FSSA/OMPP staff members should refer the requestor to the IHCP Privacy Office to obtain this form for their completion.

Accounting of disclosures

If a member requests an accounting of disclosures of their PHI made by the IHCP, any prior disclosure made pursuant to the member personal representative's request is not required to be documented in this accounting.

Note: Please refer to Section 11 of this manual, *IHCP Member Access to Protected Health Information*, for specific details.

All Other External Entities Requesting PHI Disclosure

The IHCP may disclose a member's PHI to an external entity with the appropriate authorization from the member or the member's personal representative.

In most cases, the member will request PHI disclosure from the IHCP to an external entity, such as a legislator or attorney.

Documentation Requirements

The IHCP will require that the member, or the member's personal representative, submit a written, valid authorization prior to releasing the PHI to an external entity, except under the circumstances described in Section 10 "Permitted disclosure of PHI without written authorization".

All authorizations must meet the criteria for a proper and valid written authorization.

All authorizations for the disclosure of PHI received from members or member personal representatives will be forwarded to the IHCP Privacy Office for response.

Accounting of Disclosures

If a member requests an accounting of disclosures of their PHI made by the IHCP, this accounting is not required to include any disclosure made pursuant to the member's, or the member personal representative's authorization.

Note: Please refer to Section 14 of this manual, *Member Authorization to Release Protected Health Information*, for specific details.

When member authorization is not required

The IHCP may use or disclose a member's PHI to an external entity, without the member's (or member's personal representative) authorization under specific circumstances. There are some situations in

which the IHCP is required to notify the member of the PHI use or disclosure, and some in which the member can agree to the use or disclosure. In these situations, the IHCP may provide notification verbally to the member and the member can give agreement verbally.

(Refer to Section 10 "Permitted disclosure of PHI without written authorization" for specific information).

Verification of authority

The IHCP must verify the identity of the person requesting PHI and the authority of the person to have access to PHI, if the identity or such authority of the person is not known to the IHCP.

Documentation Requirements

Also, the IHCP must obtain any documentation, statements, or representations (written) from the person requesting the PHI when the documentation, statement, or representation is required for the PHI disclosure.

If the PHI disclosure is conditioned on particular documentation, statements, or representations (written) from the person requesting the PHI, the IHCP may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that meet the requirements.

An administrative subpoena or similar process or by a separate written statement that demonstrates the applicable requirements have been met will satisfy the requirement for a disclosure for law enforcement purposes, if:

- The information requested is relevant and material to a legitimate law enforcement inquiry;
- The request is specific and limited in scope to a reasonable extent for the purpose; and
- De-identified information could not be reasonably used.

Verification of requests made by public officials

The IHCP may rely, if reasonable under the circumstances, on any of the following to verify identity when the PHI disclosure is to a public official or a person acting on behalf of the public official:

- A written statement of the legal authority under which the information is requested or an oral statement of the legal authority, if the written statement is not practical; or
- A warrant, subpoena, order, or other legal process issued by a grand

Verification of requests made by public officials (continued)

jury or a judicial or administrative tribunal if a request is made pursuant to a legal process; or

- If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status; or
- If the request is in writing, the written request is on the appropriate government letterhead; or
- If the disclosure is to a person acting on behalf of the public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency (such as a contract for services, memorandum of understanding, or purchase order), that establishes that the person is acting on behalf of the public official.
- If the public official is a legislator, authorization from the member is needed. Written requests may include a signed and authorized HIPAA compliant form or an Authorization to Act on Behalf of Constituent Form, or written correspondence or e-mail received from the constituent which includes verifiable personal information (such as social security number, case number and/or date of birth) and which clearly authorizes a Legislative (see Appendix H) staff member to receive the confidential information. In the absence of a written request, personal knowledge of the constituent's agreement to the release of the confidential information through participation in a meeting or conference call, which includes the constituent and a member of the agency's legislative team, may be sufficient.

Accounting of Disclosures

If a member requests an accounting of disclosures of their PHI made by the IHCP, these uses and disclosures will be documented on the *Accounting of Disclosures* as requested by the member, except for those cases involving:

- National security and intelligence activities; or
- Correctional institutions and other law enforcement custodial situations.

Note: Please refer to the *Uses and Disclosures of Protected Health Information When Member Authorization is not Required* Section 10 and the *Accounting of Disclosures to Member* Section 18, for specific details.

Procedure

Requests for PHI

The IHCP Privacy Office will manage all requests for copies of PHI. This includes requests for copies of PHI that may be maintained by FSSA/OMPP staff.

NOTE: Authorized staff members may continue to use and disclose PHI within the authorized, routine duties of their assigned positions. In these situations, staff members will be responsible for verification of the requestor's identification and authority prior to releasing PHI. Appropriate procedures to follow when carrying out these authorized duties are detailed throughout the appropriate sections of this manual, and in Appendix G.

Example of FSSA/OMPP staff responsibility

Member John Doe calls the staff member to ask a question regarding his PHI. Staff member Y should first verify the identity of John Doe, according to outlined procedures in this section and in *Appendix G* of this manual. Once identity is verified, staff member Y may respond to John Doe's request.

If a copy of a member's PHI is requested, the requestor should be referred to the IHCP Privacy Office.

IHCP Privacy Office
P.O. Box 7260
Indianapolis, Indiana 46207-7260

The phone number is: (317) 713-9627 or 1-800-457-4584

Deleted: 488-5018

Regulatory Requirements and Authority: 45 CFR 164.514(h)

Section 13: Member Request for Amendment of Protected Health Information

Purpose

To issue instructions to all FSSA/OMPP staff regarding the policy and procedures relating to member amendment to PHI.

Policy

Member Rights

A member has the right to request an amendment to the member's PHI or a record about the member in the designated record set from the IHCP for as long as the PHI is maintained by the IHCP. Notice of these rights and the process for the member to follow to exercise them are provided to each IHCP member in the *Notice of Privacy Practices*.

Requirements for PHI Amendment Requests

The IHCP requires that the member, or the member's personal representative, make a written request using the *Member Amendment Request* form (see Appendix D).

The IHCP will require that the request contain a statement providing a reason for the amendment, the records to be amended, and whom the member wants the IHCP to notify regarding the amendment.

Response to Amendment Requests

All requests for amendments should be referred to the IHCP Privacy Office. The Privacy Office will provide the requestor with the appropriate form, and will document, review, and respond to the requesting member within the timeframes required by the *Privacy Rule,* after receipt of the written request. The IHCP may deny a request as appropriate.

When the IHCP is not the originator of the PHI

In most instances when PHI is requested, the IHCP is not the originator of the information. In this case, the IHCP will refer the member to the healthcare provider originating the PHI. This should result in minimal amendments to PHI within IHCP.

Procedure

The IHCP Privacy Office will manage all requests from members related to the amendment of their PHI.

If a member requests that their PHI be corrected refer them to the IHCP Privacy Office.

IHCP Privacy Office
P.O. Box 7260
Indianapolis, Indiana 46207-7260

The phone number is: (317) 713-9627 or 1-800-457-4584

Deleted: 488-5018

Regulatory Requirements and Authority: 45 CFR 164.526

Section 14: Member Authorization to Release Protected Health Information

Purpose

To issue instructions to all FSSA/OMPP staff regarding the policy and procedures for acceptance of, response to, and documentation of members' authorization to release PHI.

Policy

When Member Authorization is required to use, disclose, or request PHI

The IHCP must have proper and written authorization from the member, or the member's personal representative, before the IHCP can use, disclose to, or request PHI from, another covered entity for **any purpose EXCEPT** for:

- Treatment;
- Payment;
- Health care operations; or
- As permitted or required by law without authorization (See *Uses and Disclosures of Protected Health Information When Member Authorization is Not Required,* Section 10 for additional detail).

A member's authorization is required for the use or disclosure of psychotherapy notes, with exceptions.

Use and disclosure of authorized PHI

When the IHCP obtains or receives a member's valid authorization for the IHCP's use or disclosure of PHI, the use and disclosure must be consistent with the authorization.

IHCP initiates the request for authorization

There may be rare cases in which the IHCP initiates a request for authorization from the member to release their PHI to an external entity. If the IHCP requests a member's authorization to disclose PHI to an external entity, the IHCP must return copy of the member's signed authorization form to them.

Member initiates the request for authorization

When the member requests the release of PHI to an external entity, such as a legislator or attorney, the IHCP will require that the member, or the member's personal representative, submit a written, valid authorization.

All authorizations will be documented, reviewed, and addressed by the IHCP Privacy Office. There are no set timeframes required by the *Privacy Rule* for this procedure.

Accounting of disclosures

If a member, or a member's personal representative, requests an accounting of disclosures of their PHI made by the IHCP, any disclosure made pursuant to an authorization is not required to be documented in this accounting.

Revocation of authorization

The member can, at any time, revoke all or part of their authorization by giving written notice of the revocation to the IHCP Privacy Office.

The *Right to Revoke* notice is documented in the *Notice of Privacy Practices* document and also within the *Member Authorization* form (see Appendix E).

The IHCP will require that the member submit the revocation in writing, using the *Revocation of Authorization* form.

(See Appendix E).

Procedure

Requests to release PHI

The IHCP Privacy Office will manage all requests from members related to the release of their PHI to third parties, e.g. relatives, personal representatives, member of the Legislature, etc.

If a member requests that their PHI be released to a third party refer them to the IHCP Privacy Office.

IHCP Privacy Office
P.O. Box 7260
Indianapolis, Indiana 46207-7260

The phone number is: (317) 713-9627 or 1-800-457-4584

Deleted: 488-5018

Revocation of authorization

The Privacy Office will manage all requests for revocation of authorization.

The member must submit the request to revoke authorization to the IHCP Privacy Office, in writing, as described in the *Notice of Privacy Practices* document mailed to all IHCP members. The IHCP Privacy Office, or external unit (i.e., OMPP, EDS general, HCE or ACS) will forward the *Revocation of Authorization* form to the member for completion upon request from the member. If a member submits a request for an authorization revocation, the IHCP Privacy Office will forward the *Revocation of Authorization* form to the member for completion.

The *Revocation of Authorization* form will be received in the IHCP Privacy Office, stamped with the receipt date, and logged into the Member Authorization Tracking System. If the request is received into another unit within the OMPP, EDS, or HCE, the external unit will forward the request to the IHCP Privacy Office.

The IHCP Privacy Office staff member will review the member's authorization revocation request and document the information in the Member Authorization Tracking System.

A copy of the *Revocation of Authorization Receipt* letter will be sent to the member. One copy of the response will be maintained in the Privacy Office.

> *Note: A member may revoke the authorization, in writing, at any time except to the extent that the IHCP has already taken action in reliance on the authorization.*

The authorization revocation request and response(s), including all correspondence, will be retained for six (6) years from the later of the date of creation or the date when the authorization revocation was last in effect in the IHCP Privacy Office.

Regulatory Requirements and Authority: 45 CFR 164.508

Section 15: Member Request for Alternate Communication

Purpose

To issue instructions to all FSSA/OMPP staff regarding the policy and procedures relating to members' rights relating to alternate communication requirements for PHI.

Policy

Member Rights

A member has the right to make a request to the IHCP requesting that the IHCP communicate their PHI to them in a certain way or at a certain location. Notices of these rights and the process for members to follow are provided to each IHCP member in the *Notice of Privacy Practices* document.

How to request alternate communication

The IHCP will require that the member, or the member's personal representative, make a written request using the *Alternate Communication Request* form (see Appendix F).

All requests for alternate communication of PHI will be documented, reviewed, and responded to the requesting member within the timeframes required by the HIPAA *Privacy Rule*.

Requirements of the IHCP in approval or denial of requests

The IHCP must accommodate reasonable requests for communicating with a member by alternate means at alternate locations, if the member clearly states that the disclosure of all or part of the PHI could endanger the member.

The IHCP may approve or deny alternate communication requests and is not required to agree to a confidential communication request unless the member indicates endangerment.

If the IHCP agrees to communicate with the member through alternate means, it must communicate as agreed upon with the member in order not to violate the agreement.

Procedure

Right to request alternate communication	Members have a right to request that their information, such as the NPP or copies of their PHI, be sent to them in an alternative manner or to an alternative location, relative to the standard method of providing this information to them.
Examples of alternate communication	This may take the form of requesting electronic copies instead of paper or that the information be mailed to an address other than the address on the eligibility file.
Requests for alternate communication	Any requests from members for alternate communication should be referred to the IHCP Privacy Office. IHCP Privacy Office P.O. Box 7260 Indianapolis, Indiana 46207-7260 The phone number is: (317) 713-9627 or 1-800-457-4584

Deleted: 488-5018

Regulatory Requirements and Authority: 45 CFR 164.522(b)

Purpose

To issue instructions to all FSSA/OMPP staff regarding the policy and procedures for acceptance of, response to, and documentation of members' complaints about alleged violations of their rights relating to PHI.

As a covered entity under HIPAA, the IHCP must provide a process for a member to make complaints concerning its privacy policies and procedures, as well as its compliance with these policies and procedures. This policy and procedure document sets forth that process for the IHCP.

Policy

Member Rights

A member of IHCP has the right to file a complaint to the IHCP and to the Secretary if they believe that their privacy rights have been violated.

In addition, the member has the right to file a complaint with the Secretary of HHS if they believe that the IHCP is not complying with the applicable requirements of the *Privacy Rule*.

Notice of these rights and the process for the member to follow to exercise them are provided to each IHCP member in the *Notice of Privacy Practices*.

Filing a Complaint

The IHCP will suggest the member to file the complaint with the IHCP Privacy Office in writing and within 180 days of the incident for which the complaint is being registered.

Requirements of the IHCP

All complaints received will be documented and investigated, and a response provided to the complainant, with a copy provided to the OMPP Privacy Coordinator.

The IHCP will not take any retaliatory action against a member who has filed a complaint with the IHCP or with the Secretary of HHS.

Procedure

Member complaints regarding use of their PHI

The IHCP Privacy Office will be responsible for receiving, reviewing, and responding to complaints from members regarding use of their PHI.

If a member complains that the IHCP has misused their PHI please refer them to the IHCP Privacy Office.

IHCP Privacy Office
P.O. Box 7260
Indianapolis, Indiana 46207-7260

The phone number is: (317) 713-9627 or 1-800-457-4584

Deleted: 488-5018

Regulatory Requirements and Authority:
45 CFR 164.520(b)(1)(vi)
45 CFR 164.530(d)(1)

Section 17: Member Request to Restrict Protected Health Information

Purpose

To issue instructions to all FSSA/OMPP staff regarding the policy and procedures for acceptance of, response to, and documentation of members request to restrict uses and disclosures of PHI.

Policy

Member Rights

A member has the right to request that the IHCP to restrict the uses and disclosures of his or her PHI as it relates to treatment, payment, or health care operations and other disclosures permitted by the *Privacy Rule.*

Notices of these rights and the process for the member to follow are provided to each IHCP member in the *Notice of Privacy Practices* document.

How to request a restriction on use of PHI

The IHCP will require that the member, or the member's personal representative, make a written request for a restriction and to specify the type of information to be included in the restriction, to whom the restriction applies, and the effective dates of the restriction period.

See Appendix J to access the *Member Restriction Request Form.*

IHCP Authority

The OMPP Privacy Coordinator has the authority to approve or deny restriction requests. The IHCP is not required to agree to a restriction; however, if the IHCP agrees to a restriction, it may not use or disclose the PHI to the restricted parties without violating the restriction.

Required exclusions to restricted use

A restriction agreed to by the IHCP does not prevent the uses or disclosures of PHI that are permitted or required as follows:

- When required by the Secretary to investigate or determine the IHCP's compliance with the *Privacy Rule*;
- For public health activities if required by law;
- To other government agencies providing benefits or services to the individual;
- To government agencies that oversee health care programs;
- For research (if related to a State Plan purpose); and
- For other uses and disclosures that are required by law.

Refer to the *Uses and Disclosures of Protected Health Information When Member Authorization is Not Required*, Section 10, for specific activities permitted or required by law for the IHCP to use or disclose PHI.

Termination of Restriction

The IHCP may terminate its agreement to a restriction, if:

- The member agrees to or requests the termination in writing;
- The member orally agrees to the termination and the oral agreement is documented; or
- The IHCP informs the member that it is terminating its agreement to a restriction, except that such termination is only effective with respect to PHI created or received after it has so informed the member.

Procedure

Requests for restricted use of PHI

The IHCP Privacy Office will manage all requests from members to restrict the use of their PHI.

If a member requests that the use of their PHI be restricted refer them to the IHCP Privacy Office.

IHCP Privacy Office
P.O. Box 7260
Indianapolis, Indiana 46207-7260

The phone number is: (317) 713-9627 or 1-800-457-4584

Deleted: 488-5018

Regulatory Requirements and Authority:
45 CFR 164.522(a)
45 CFR 164.502(c)

Section 18: Accounting of Disclosures to Member

Purpose

To issue instructions to all FSSA/OMPP staff regarding the policy and procedures relating to the accounting for disclosures, to IHCP members, of their PHI.

Policy

Requirements of the IHCP

The IHCP must account to an IHCP member, or a member's personal representative, for PHI disclosures, as required by the *Privacy Rule* for those instances in which the PHI is released to an external entity for purposes other than treatment, payment, or health care operations.

When an accounting of disclosures is not required by the IHCP

The majority of PHI received and disclosed by the IHCP is used for treatment, payment, and operations, so the disclosure of PHI for other purposes should be minimal. The IHCP **is not required** to account for disclosures:

- To carry out treatment, payment and health care operations;
- To IHCP members (for PHI about them);
- To a member's personal representative;
- To correctional institutions or law enforcement officials; or
- That occurred prior to the compliance date (April 14, 2003).

When an accounting of disclosures is required by the IHCP

The IHCP **will be required** to account for disclosures, such as those:

- For research;
- To other government agencies providing benefits or service to members, or that oversee health care providers (if the disclosure does not meet the definition of treatment, payment, or health care operations); or

- Any other disclosure that is not identified as being excluded above.

Documentation Requirements	Disclosures that require an accounting must be documented so that an accounting can be provided to the member if requested. All requests for accounting of disclosures will be documented, reviewed, and responded to within the timeframes required by the *Privacy Rule*. Refer to Appendix K for the *Member Accounting Request Form*.
Availability of historical disclosures	The disclosure of a member's PHI must be accounted for six years and will commence April 14, 2003. The member can request a six-year history, but this cannot be created for disclosures prior to the April implementation date.
Cost per disclosure accounting	The IHCP will provide one free disclosure accounting per member each 12 months. The IHCP may charge the member for each additional disclosure accounting during the same 12-month period.
Additional Information	IHCP Privacy Office staff members will follow the policies and procedures contained in their manual to comply with the *Privacy Rule* for uses and disclosures of PHI. See the *Permitted and Required Uses and Disclosures of Protected Health Information*, Section 3, for additional information.

Procedure

Required Documentation	Any PHI that is released to any person or entity, other than the member, for purposes other then treatment, payment, or healthcare operations (TPO) must be documented and an accounting provided to the member, if requested by the member, for up to six years, beginning April 14, 2003. See the *Glossary* section of this manual for a detailed description of TPO.
Release of PHI	FSSA/OMPP staff members **are not** authorized to release any PHI for purposes other than TPO, unless they have been approved to do so, and such release has been coordinated with the OMPP Privacy Coordinator.

Requests for Accounting of Disclosures

If a member requests an accounting of disclosures of their PHI, they must complete a *Member Accounting Request Form* (provided in Appendix K of this manual), and submit the completed form to the IHCP Privacy Office.

IHCP Privacy Office
P.O. Box 7260
Indianapolis, Indiana 46207-7260

The phone number is: (317) 713-9627 or 1-800-457-4584

Deleted: 488-5018

Charging the Member for Accounting of Disclosure Copies and Mailings

If the accounting of disclosures request from the member or member's personal representative meets the criteria for charging, the member or personal representative must be notified in writing of the charge prior to the accounting copying and mailing. The *Disclosure Accounting* letter will be mailed to the member to provide the copying and mailing charges that would result from the accounting request.

The member is instructed to contact the IHCP Privacy Office to make arrangements. A personal check or money order will be accepted as payment. All payments received into the IHCP Privacy Office will be tracked and be forwarded to the EDS Finance Unit for deposit.

Suspended Rights

The IHCP must temporarily suspend a member's right to receive an accounting of disclosures made to a health oversight agency or law enforcement official, for the time specified by such an agency or official, if the agency or official provides the IHCP with a written statement that such an accounting to the member would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

Regulatory Requirements and Authority: 45 CFR 164.528

Section 19: Safeguards for Staff use of Protected Health Information Access

Purpose

To issue instructions to all FSSA/OMPP staff regarding the policy and procedures relating to workforce members access to, and use of, IHCP members' PHI.

Policy

Requirements of the IHCP: Access Limitations

The *Privacy Rule* requires that safeguards be in place to limit unnecessary or inappropriate access to protected health information. To be in compliance, the IHCP must apply the minimum necessary requirements, including access and use by the FSSA/OMPP staff and contractor staff, for most PHI uses and disclosures.

The IHCP shall limit access and use of PHI by its staff and contractors to the minimum necessary to accomplish the defined work functions.

The requirements also apply to PHI requests made by, or on behalf of, the IHCP to another covered entity.

The access limitations apply to all paper, fax, oral, and electronic communication of PHI. This is inclusive of IndianaAIM along with any other database or repository of information containing PHI.

Exclusions to access limitation requirements

There are instances in which the minimum necessary limitation is not required, including:

- Disclosures made to a member's health care provider for the purpose of providing treatment;
- Disclosures made to the member or through the member's written authorization in regard to their own PHI; or
- Uses or disclosures required by law, including the HIPAA *Privacy Rule*.

Refer to Section 4 of this manual, *Minimum Necessary Requirements*, for additional information.

Procedure

Paper Communication

All paper communication that contains PHI, to any entity outside of the IHCP, must be contained within a sealed envelope or other protective cover to prevent the inadvertent disclosure of PHI to an unauthorized person. This includes courier service to EDS or HCE, mail to IHCP providers or members, PHI forwarded to other IHCP contractors, or any other entity that has been authorized to receive the PHI.

Hard copy documents containing PHI must be protected as described in the *Protected Health Information Safeguards* section of this manual. FSSA/OMPP staff members who are not required to use PHI in their work functions are prohibited from PHI access, unless prior approval has been received from their direct supervisor.

Fax Communication

All fax communication containing PHI, provided to any entity outside of the IHCP, must be accompanied by a cover sheet containing the statement:

"This facsimile transmission (and attachments) may contain protected health information from the IHCP, which is intended only for the use of the individual or entity named in this transmission sheet. Any unintended recipient is hereby notified that the information is privileged and confidential, and any use, disclosure, or reproduction of this information is prohibited. Any unintended recipient should contact Jenifer Nelson, OMPP Privacy Coordinator, by telephone at (317) 233-0446 immediately."

Fax documents containing PHI must be protected as described in the *Protected Health Information Safeguards* section of this manual. FSSA/OMPP staff members who are not required to use PHI in their work functions are prohibited from PHI access, unless prior approval has been received from their direct supervisor.

Oral Communication

All oral communication concerning a member's PHI must be limited to the nature of the intended work and will only be discussed in the appropriate area within the IHCP. No PHI communication of any type is to be discussed outside of the IHCP workspace, including other areas within the building complex.

E-Mail Communication

PHI communicated via e-mail text or attachments, to any FSSA/OMPP staff member or external entity, should always be limited to the minimum necessary amount of information that is needed exclusively to carry out treatment, payment, or operations (TPO). E-mail transmissions of PHI must only be made to individuals who are authorized to receive such information, and files containing PHI that are exchanged with outside entities (i.e., outside of the secure State network) should be encrypted with the "Certified Mail" tool, or the currently approved OMPP encryption tool. In addition, the following statement will be systematically generated at the bottom of all email messages:

"The information contained in this E-mail and/or attachments may contain protected health, legally privileged, or otherwise confidential information intended only for the use of the individual(s) named above. If you, the reader of this message, are not the intended recipient, you are hereby notified that you may not further disseminate, distribute, disclose, copy or forward this message or any of the content herein. If you have received this E-mail in error, please notify the sender immediately and delete the original."

All questions concerning e-mail transmission of PHI are to be referred to the OMPP Privacy Coordinator for resolution.

Indiana*AIM* Access

On a periodic basis, all IHCP management staff will review the quarterly Indiana*AIM* class summary for their business unit, in relation to PHI access via Indiana*AIM,* in order to answer the following questions:

- Are the Indiana*AIM* profiles for the workforce classes in their respective units, specifically those that provide access to member PHI, still necessary for staff to perform their work functions?
- Are the actual Indiana*AIM* access classes currently assigned to the staff members in their units the same in comparison to the pre-assigned profiles for the workforce class for each staff member?
- Are all staff members assigned to the unit classes currently working in the unit?
- Are any staff members who currently work in the unit, but are not listed on the quarterly profile for the business unit, assigned to another unit's access class?

Modification to Indiana*AIM* classes

For any change needed to modify the Indiana*AIM* access profiles for the work unit, the IHCP manager will notify the OMPP Privacy Coordinator of the needed change. No action is necessary if no changes are recommended.

For any staff member found to be on the unit access profile who is not currently working in the unit, notify the OMPP Privacy Coordinator of the need to delete all Indiana*AIM* access for that staff member. Also notify the staff member's current manager of the access deletion and the need to request the appropriate Indiana*AIM* access for the new job function.

For any staff member who is not found to be on the unit access profile, forward the appropriate Indiana*AIM* access profile request for the staff member to the EDS Security Unit.

Regulatory Requirements and Authority:
45 CFR 164.514(d)(2)(i)
45 CFR 164.530(c)(1)

Section 20: Protected Health Information Safeguards

Purpose

To issue instructions to all FSSA/OMPP staff regarding the policy and procedures relating to the:

- administrative,
- technical, and
- physical safeguards

to adequately protect IHCP members' PHI.

Policy

Responsibility of FSSA/OMPP Staff

It is the responsibility of all FSSA/OMPP staff and contractor staff to reasonably protect all members PHI from inappropriate use or disclosure.

OMPP is housed in a secure self-contained area. OMPP workforce members are authorized to enter this area through one of three doors, which require a four-digit access code for entrance. Each individual OMPP staff member has a unique access code that permits entrance into the facility. The access code is not to be shared with anyone else.

Visitor controls are in place to limit outside entrance into facilities. Visitors may enter the OMPP facility through one door, which is monitored during all operating hours by a receptionist. There is a waiting area with available seats for guests; seats are positioned away from areas where PHI could be visible. Visitors must be approved for entrance, sign a log of visitation, wear a visitation badge and be escorted by an authorized OMPP staff member at all times.

Types of Member PHI Requiring Safeguards

All IHCP members PHI in written, electronic, or oral form is protected by the *Privacy Rule* and must be safeguarded in the work place and in the daily job functions of all FSSA/OMPP staff members.

This includes PHI access through the IHCP office or through off-site access.

Unauthorized use or disclosure of PHI by FSSA/OMPP staff	Any unauthorized use or disclosure by an FSSA/OMPP staff member will be subject to the sanctions set forth by the IHCP for breach of security or privacy. Refer to Section 21, *Sanctions*, for additional details.

Procedure

FSSA/OMPP Staff Responsibilities	All FSSA/OMPP staff are responsible to help ensure that the appropriate administrative safeguards are followed to protect against the unauthorized use of a member's PHI. All OMPP staff are also responsible for assisting in controlling and validating a person's access to facilities.
Work Station Requirements	FSSA/OMPP staff are to maintain a secure personal working environment that: • Safeguards PHI while they are not at their station; • Maintains the positioning of their computer screen to ensure that PHI is protected from unauthorized viewing; • Implements password protection controls as required by DTS; • Removes records containing PHI from desktops and places such records in locked drawers or file cabinets; • Ensures that all drawers containing PHI are closed and locked; • Ensures that PHI is not left unattended in the aisles; and • Does not allow unauthorized visitors into the IHCP work area.
Disposal of documents containing PHI	FSSA/OMPP staff must ensure that paper documents containing PHI are shredded prior to their disposal.

Regulatory Requirements and Authority:
45 CFR 164.514(d)(2)(ii)
45 CFR 164.530(c)(1-2)

Purpose

To issue instructions to all FSSA/OMPP staff regarding the policy and procedures relating to sanctions against workforce members who fail to comply with the established privacy policies and procedures.

Policy

Sanctions against IHCP workforce members

The IHCP is required to develop, and apply when appropriate, sanctions against members of its workforce who fail to comply with privacy policies or procedures or with the requirements of the *Privacy Rule*.

Types of Sanctions

The IHCP is required to develop and impose sanctions appropriate to the nature of the violation.

The type of sanction may vary depending on factors such as the severity of the violation, whether the violation was intentional or unintentional, and whether the violation indicates a pattern or practice of improper use or disclosure of PHI.

Sanctions could range from a warning to termination.

These sanctions do not apply to whistleblower activities.

Documentation Requirements

The IHCP is required to have written policies and procedures for the application of appropriate sanctions for violations of the *Privacy Rule* and to document those sanctions.

Documentation must be retained for six years by the Privacy Coordinator.

Procedure

FSSA/OMPP staff violation of the *Privacy Rule*	FSSA/OMPP staff who violate the privacy requirement of HIPAA are subject to appropriate sanctions which may include suspension or termination. Sanctions will be imposed in accordance with FSSA guidelines.
Mitigation	Pursuant to 45 CFR 164.30(f), the IHCP must mitigate, to the extent practicable, any harmful effect that is known from any use or disclosure of PHI, by a staff member or a business associate of the IHCP, in violation of IHCP policies and procedures, or the requirements of the *Privacy Rule*.

Regulatory Requirements and Authority: 45 CFR 164.530(e)

Purpose

To provide instructions for the IHCP in regard to the training of all FSSA/OMPP staff in regard to HIPAA privacy regulations.

Policy

The OMPP Privacy Coordinator will ensure that all FSSA/OMPP staff receive training, and periodic re-training, on HIPAA policies and procedures as necessary and appropriate for their function with IHCP.

Procedure

Training and certification of FSSA/OMPP Staff	The OMPP Privacy Coordinator is responsible for ensuring that all FSSA/OMPP staff are trained concerning privacy requirements.
Documentation	The OMPP Privacy Coordinator will maintain all records to document this training.
Existing FSSA/OMPP Staff	The OMPP Privacy Coordinator will ensure that all existing FSSA/OMPP staff receive privacy training and obtain a passing score on the post-training evaluation.
New FSSA/OMPP Staff	The OMPP Privacy Coordinator will ensure that all new FSSA/OMPP staff are provided with the privacy training module and obtain a passing score on the post-training evaluation.
Re-training Requirements	On a periodic basis, the OMPP Privacy Coordinator will arrange for IHCP-wide privacy re-training.

Regulatory Requirements and Authority: 45 CFR 164.530(b)

Business Associate

A person or organization that performs a function or activity on behalf of the IHCP but is not a part of the FSSA/OMPP staff such as EDS, Health Care Excel (HCE), or Myers and Stauffer.

Covered Entity

A *covered entity* is a health plan, health care clearinghouse, or any health care provider who transmits any health information in an electronic form in connection with any HIPAA-required transactions. This includes the use of the OMNI device or direct data entry (Web entry) by a provider. Medicaid is specifically mandated as a health plan in the Act.

Data Use Agreement

The agreement between the IHCP and the limited data set recipient, those receiving de-identified data, to obtain satisfactory assurance that the limited data set will only be used or disclosed for limited purposes. The data use agreement content must:

- Establish the permitted uses and disclosures of the information by the limited data set recipient, which can only be for research, public health, or health care operation purposes;
- Not allow use or further disclosure by the limited data set recipient outside of the scope of the uses authorized by the *Privacy rule*;
- Establish who is permitted to use or receive the limited data set; and
- Provide that the limited data set recipient will:
  - Not use or disclose the information other than permitted by the data use agreement or as required by law;
  - Use appropriate safeguards to prevent use or disclosure that is not permitted by the data use agreement;
  - Report to the IHCP any use or disclosure of the limited data set that is not permitted by the data use agreement as it becomes aware of such violation;
  - Ensure that any agents, including subcontractors abide by the same restrictions and conditions that apply to the limited data set recipient, in regard to the limited data set usage; and
  - Not identify the information or contact the individuals.

Designated Record Set

The *designated record set* defines the scope of information that the IHCP member has the right to access and request amendment. The designated record set is not required to reside in one location. If a business associate of the IHCP, such as EDS or HCE, maintain the information, it is still considered to be part of the IHCP designated record set.

As a health plan, the IHCP creates the claim records from information received from a health care provider and creates the eligibility file from information received via the ICES system. The individually identifiable information maintained in the electronic claims subsystem and eligibility subsystem, for the specific member, are considered the individually identifiable information in the IHCP's designated record set.

Information maintained by the IHCP in regard to eligibility determination, program coverage decisions, or payment are considered to be a part of the designated record set. Copied information that is forwarded to the IHCP, when the original is kept by the author, is considered part of the designated record set, and thus, would be accessible to the member through the IHCP.

Designated record set means: A group of records maintained by or for a covered entity that is:

- The medical records and billing records about individuals maintained by or for a covered health care provider;
- The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
- Used, in whole or in part, by or for the covered entity to make decisions about individuals (with the exception of psychotherapy notes).

With some exceptions noted in the IHCP *Member Access to Protected Health Information* policy, the Medicaid member has the right to access their PHI contained and maintained in the designated record set.

IHCP Designated Record Set

The IHCP designated record set consists of information used to provide treatment and payment for the provision of healthcare. This information would be contained in:

- Electronic claim records maintained in the Indiana*AIM* claim subsystem
- Member Eligibility information in the Indiana*AIM* recipient subsystem
- Original paper Prior Authorization records
- Original Third Party Liability records
- Original medical records used by the IHCP to make decisions about the member, such as the *Determination of Disability Medical Information* form used by the Medical Review Team for Medicaid eligibility determination.

What is not in the Designated Record Set

Information used for operational purposes, is not included in the designated record set, such as:

- Case management and care coordination
- Medical review
- Fraud and abuse detection
- Compliance programs

Encryption

Encryption is the conversion of data into a form, called a ciphertext that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be

understood.

IndianaAIM

IndianaAIM is Indiana's Medicaid Management Information System. In addition to performing claims processing, the system maintains extensive recipient and provider information online, real time for eligibility verification and payment status information. IndianaAIM also includes a Decision Support System, which enables staff to access and retrieve data from multiple databases and create reports online.

Limited Data Set

A *limited data set* is PHI that excludes direct identifiers of the individual or of relatives, employers, or household members of the individuals. The direct identifiers to be excluded to constitute a limited data set include:

- Names;
- Postal address information, other than town or city, State, and zip code;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate /license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints; and
- Full face photographic images and any comparable images.

IHCP Limited Data Set

The Indiana Health Coverage Programs (IHCP) does not collect all of the identifiers that are to be removed from the PHI to create a limited data set. For the IHCP limited data set purpose, the following identifiers would be removed from the PHI:

- Name;
- Medical record number (if applicable);
- Postal address information, other than town or city, State, and zip code;
- Telephone number;

- Social security number;
- Health plan beneficiary numbers (the member's RID information); and
- Account number (if applicable).

The IHCP may use or disclose a limited data set of PHI if the IHCP enters into a Data Use Agreement with the limited data set recipient. The limited data set and this agreement can only be used for the following purposes:

- Research,
- Public health, or
- Health care operations.

Personal Representative

An individual who, under state law, has the authority to act on behalf of a member.

Protected Health Information

Protected health information (PHI) is the individually identifiable health information that is:

- Transmitted by electronic media, which includes Internet, Extranet, leased lines, dial-up lines, private networks, magnetic tape, disk, or compact disk (45 CFR 162.103);
- Maintained in any electronic media; or,
- Transmitted or maintained in any other form or medium, which include oral communication or paper.

The IHCP is responsible for protecting the IHCP member's PHI in regard to access for use or disclosure. The majority of member information maintained on the IndianaAIM Recipient and Claim subsystems would qualify as PHI, and access must be limited to only those IHCP and contractor staff who require PHI usage in order to carry out their daily work duties. Full-time access or part-time access of limited duration, as in the case for special project work, may only be granted by the employee's supervisor and will be monitored by the supervisor on a quarterly basis.

Individually Identifiable Health Information

Individually Identifiable Health Information is a subset of health information, including demographic information collected from the member, and:

- Is created or received by a health care provider health plan, employer, or health care clearinghouse; and
- Relates to the past, present, or future physical or mental health or condition of an member; the provision of health care to a member; or the past, present, or future payment for the provision of health care to a member; and

- That identifies the member; or
- Could reasonably be used to identify the member.

Health information includes information, whether oral or recorded in any form or medium.

PHI Exclusions

PHI excludes the individually identifiable health information in:

- Education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232g;
- Records used exclusively for health care treatment, for students 18 years or older or that are held by a post-secondary educational institution, and that have not been disclosed other than to a health care provider at the student's request; and
- Employment records held by a covered entity in its role as an employer.

Treatment, Payment, and Health Care Operations

The IHCP may use and disclose PHI to carry out the treatment, payment, and health care operation functions, as defined, without authorization from the IHCP member. The information may not be used for any other purposes, such as holiday greetings, general public announcements, partisan voting information, or alien registration notices.

Except in the use and disclosure for treatment purposes, the IHCP must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request when using, disclosing, or requesting PHI from another covered entity.

The FSSA/OMPP staff or contractor staff must ensure that the requesting covered entity has the authority to request and obtain the member's PHI.

Treatment

Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including:

- The coordination or management of health care by a health care provider with a third party;
- Consultation between health care providers relating to a patient; or
- The referral of a patient for health care from one health care provider to another.

The IHCP does not provide direct treatment to members. However, appointment reminders and referrals to health care providers are considered treatment activities under HIPAA. The IHCP may disclose PHI to a member's treating provider to enable the member to receive health care.

NOTE: The *minimum necessary* requirement does not apply to disclosures to

or requests by a health care provider for treatment.
(45 CFR 164.502(b)(2)(i))

Payment

Payment means the activities that relate to the individual to whom health care is provided undertaken by:

- A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or
- A health care provider or health plan to obtain or provide reimbursement for the provision of health care.

Payment activities include, but are not limited to:

- Determination of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), such as:
  - Eligibility determinations made by, or on behalf of, the OMPP by other agencies for low-income families; pregnant women; children in foster care; aged, disabled, or blind individuals; and individuals residing in state institutions,
  - Data exchanges with the Social Security Administration to identify SSI recipients and perform Medicare buy-in activities for dually-eligible members,
  - Resolution of enrollment errors,
  - Production of ID cards,
  - Provision of enrollment, disenrollment, and error lists to the managed care organizations,
  - Verification of IHCP eligibility, coverage type, and service limitations to IHCP health care providers,
  - Data exchange with the Internal Revenue Service (IRS) to verify member income and assets for eligibility determination, and
  - Estate recovery, after a member's death, for those amounts paid by Medicaid on the member's behalf after they reached age 55.
- Adjudication or subrogation of health benefit claims;
- Risk adjusting amounts due based on enrollee health status and demographic characteristics;
- Billing, claims management, collection activities, obtaining payment under a contract for reinsurance, and related health care data processing;
- Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; and
- Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services, including:
  - Member assessment for long term care or waiver program placement, and
  - Prior authorization of IHCP services.

Health Care Operations

Health care operations means any of the following activities performed by the covered entity:

- Conducting quality assessment and improvement activities, including:
  - Outcomes evaluations and development of clinical guidelines,
  - Activities related to improving health or reducing health care costs,
  - Case management and care coordination,
  - Contacting health care providers and patients with alternative treatment information, and
  - Related functions that do not include treatment;
- Reviewing the qualifications or competence of health care professionals, evaluating performance, training, accreditation, certification, licensing, or credentialing activities;
- Underwriting, premium rating, or other work in regard to health insurance or health benefits, including:
  - Establishing managed care capitation rates,
  - Fee schedules, and
  - Payment amounts for services rendered to IHCP members;
- Conducting or arranging for medical review, legal services, and auditing functions, including:
  - Fraud and abuse detection, and
  - Compliance programs;
- Business planning and development activities, including:
  - Policy development for covered services, guidelines, limitations, and protocols,
  - Review and approval of the preferred drug list (PDL), and
  - Budget forecasting and expenditure analysis; and
- Business management and general administrative activities of the covered entity, including:
  - Customer service functions for applicants, members, and providers,
  - Complaint and problem resolution, and
  - De-identification of data.

Unemancipated Minor Minor who is less than 18 years of age, and is either living with, or financially dependent upon a parent/legal guardian.

Appendix A: Notice of Privacy Practices

Note: Notice is effective April 14, 2003. This is not the official form. For an official form, please contact the IHCP Privacy Office.

Indiana Health Coverage Programs

NOTICE OF PRIVACY PRACTICES

If you would like a copy of this notice in Spanish, please contact the IHCP Privacy Office at (317) 713-9627 or 1-800-457-4584

Si usted desea una copia de esta noticia en Español, por favor contacte a la Oficina Privada de IHCP al (317) 713-9627 o al 1-800-457-4584.

This notice is to all Indiana Health Coverage Programs (IHCP) members including Medicaid, Hoosier Healthwise, Medicaid Select, and members residing in institutions operated by the Indiana State Department of Health and the Division of Mental Health and Addictions who have received medical services outside of those institutions. This notice is for your information only. You do not need to take any action as a result of this notice.

Notice of Privacy Practices

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

This notice tells how the IHCP may use or release your health information. It also tells you about your rights and the IHCP requirements about the use and release of your health information. Your health information will not be shared without your written authorization except as described in this notice, or when required or permitted by law. If you give us your written authorization, you may change your mind by telling us in writing. The IHCP may change its privacy practices and make the new privacy practices effective for all protected health information we maintain. If the terms of this notice change we will mail you a revised copy of this notice to the address you have supplied.

Our Responsibilities and Commitment to You

We understand that your health care information is personal. We take our responsibility to keep your personal health information private very seriously. We are committed to following all state and federal laws that protect your health information. We are required to protect your health information, tell you about your rights to your health information, and to give you this notice explaining our responsibilities and the ways we use and share your health information.

Use and Disclosure of Your Health Information

We do not create health records. We receive health information to help us make decisions about whether you qualify for certain programs or services. We use your health information to pay for services provided to you by your health care provider, for health care operations, and to evaluate the quality of services you receive. While we cannot describe all cases related to the use of your health information, the following are some common examples of how we use your personal health information:

- Doctors, hospitals, and other health care practitioners that provide services to you submit your health information to us in the form of a claim for payment. They may also give us your health information in order to obtain prior authorization or to find out if a service is covered. These requests include information that identifies you, your diagnosis, and procedures you have received, or that you might receive in the future. We use this health information to approve and pay for the services that we cover. We may also share your information with other programs that may pay for your health care, such as Medicare or private insurance companies in order to get payments.
- We may use your health information to review the care and outcome of your treatment and to compare the outcomes of other people who received the same or similar treatment. We use this information to improve the quality and effectiveness of health care services.
- We may also disclose your health information to our employees, as well as companies and persons we have contracts with, so they can perform the jobs we ask them to do, such as approving services for you or reviewing payments made to health care practitioners. To protect your health information we require everyone who has a contract with us to follow rules protecting your information.
- We may use and disclose your health information to tell you or your provider about possible treatment options, alternative treatments, and for other health-related benefits.
- We may disclose or share your health information with other government agencies that may provide public benefits or services to you. We may also disclose or share your information with other government agencies permitted by law, including the federal government, to show how the IHCP is working and to improve the programs.

- We may use or disclose your health information in compliance with the law in a public emergency to notify your family, for public health activities to prevent or control disease, injury or disability or report abuse, to comply with Workers' Compensation laws, as required by law including in response to a subpoena, discovery request, court or administrative order, for issues of national security, to report vital statistics, or to process organ donation information.
- We may disclose your information to researchers when the information cannot identify you or when their research has been reviewed and approved by an institutional review board to ensure the continued privacy and protection of your health information.

Your Health Information Rights

- You have the right to request that the IHCP not release your personal health information, release only part of your information, or release it for reasons you request. We are not required to honor your request.
- You have the right to request a paper copy of this notice at any time, even if you agree to receive it electronically by e-mail.
- You have the right to request a list showing each time we released your personal health information. Your written request must be submitted to the IHCP Privacy Office and state what time period you want to cover. The time period may not go back further than six years and may not include dates before April 14, 2003. This list will not include personal health information that was released to provide treatment to you, to make or obtain payment for services, for health care operations, for national security, or for use by prisons or law enforcement officials. This list will not include information released to you by the IHCP that you requested in writing, or information released to persons who are involved in your care.
- You have the right to request that we contact you about your personal health matters in a certain way or at a certain location. For example, you can request that we only contact you at work or by e-mail. We will review and accommodate only reasonable requests. To request a special way or location for us to contact you about your personal health information, you must write to the IHCP Privacy Office at the address in the contact information at the end of this notice.
- You have the right to see and get a copy of your health information. You may be charged a fee for the costs of copying, mailing, or for other supplies needed for your request. You do not have the right to see or copy information used for lawsuits, criminal investigations or prosecutions, or notes made by a mental health therapist or psychiatrist. If you ever feel you have not been allowed to see or have copies of your medical information you can file an appeal with the IHCP Privacy Office. If an appeal is filed with the IHCP Privacy Office, an individual who did not participate in the decision to deny the request will review the appeal.
- You have the right to ask that we change health information that you feel is incorrect or incomplete. Your request may be denied if we did not create or write the information, it is not part of the information you can see or copy, or if we decide the personal health information has no errors and is complete.

Note: All requests about your health information must be in writing and sent to the IHCP Privacy Office address listed in the contact information section at the end of this notice.

Contact Information or Filing a Complaint

If you have questions or want additional information, you can contact the IHCP using the following address or phone number.

If you have a complaint about our health information practices or believe that we have violated your privacy rights, please submit the complaint to the IHCP at the following address. **All complaints must be submitted in writing.**

IHCP Privacy Office
P.O. Box 7260
Indianapolis, IN 46207-7260
(317) 713-9627 or 1-800-457-4584

You can also file a complaint with the Secretary of Health and Human Services at the following address.

Secretary of Health and Human Services
200 Independence Avenue, SW
Washington, D.C. 20201

We will never take action against you for filing a complaint and it will not impact the health care services provided to you.

Appendix B: Member Access Request Form

Please click on the following link to access the Member Access Request Form:

Form SF51737

Appendix C: Verification of Identity and Authority Form

Note: This is not the official form. For an official form, please contact the IHCP Privacy Office.

Formatted: Highlight

Verification of Identity and Authority Form – For EDS Internal Use Only

This form is used to document your verification of the identity and authority of a person or entity, unknown to you, before granting access to or disclosing protected health information.

Section A: Member whose information is being disclosed

Name: _____

Address: _____

City, State, ZIP Code: _____

IHCP RID Number: _____ Phone Number: _____

Section B: Identity of person to whom information is being disclosed

Obtain a copy of what you relied upon to identify the person. Attach the copy to this form.

Name: _____

Company, organization, or government agency with whom the person claims affiliation:

_____

Address: _____

City, State, ZIP Code: _____

Phone Number: _____ E-mail: _____

Personal representative's relationship to member:

_____

☐ Person is known to me. Explain how you know the person:

_____

_____

☐ Personal identification (*e.g.* driver's license, photo ID). What document did you see?

_____

_____

☐ Government credentials (*e.g.* badge, identification card, appropriate document on government letterhead). What document did you see?

(Form continued on Page 2)

Section C: Authority of person to receive access to protected health information being disclosed

Obtain a copy of what you relied upon to authorize the person. Attach the copy to this form.

☐ Authority is known to me. Explain basis of your knowledge:

_____

_____

☐ Personal representative status (*e.g.* identification as parent, guardian, executor, administrator, power of attorney). Copy of document attached.

_____

_____

☐ Warrant, subpoena, order, summons, civil investigation demand or other legal process. Copy of document attached.

_____

_____

☐ Appropriate document on government letterhead. Copy of document attached.

_____

_____

☐ Government official's oral representation. State what you were told and why your reliance on it was reasonable under the circumstances:

_____

_____

_____

Section D: Signature

Form completed by:

Signature: _____ Date: _____

Attach this form to the verification documentation you obtained.

Appendix D: Member Amendment Request Form

Please click on the following link to access the Member Amendment Request Form:

Form SF51739

Appendix E: Member Authorization and Revocation Form

Please click on the following link to access the Member Authorization and Revocation Form:

Form SF51733

Appendix F: Alternate Communication Form

Please click on the following link to access the Alternate Communication Form:

Form SF51741